PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-094549
(43)Date of publication of application : 06.04.2001

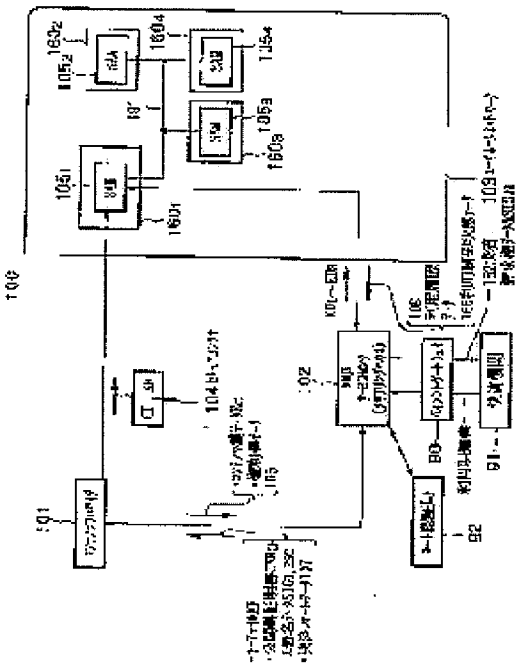
(51)Int.Cl. H04L 9/08
G06F 12/14
G06F 15/00
G09C 1/00
G11B 20/10
H04L 9/32

(21)Application number : 11-309721
(22)Date of filing : 17.09.1999

(71)Applicant : SONY CORP
(72)Inventor : NONAKA SATOSHI
EZAKI TADASHI

(54) DATA PROVIDING SYSTEM AND ITS METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a data providing system which can protect the profit of persons concerned in a data providing device.
SOLUTION: An EMD service center 102 generates a stored key file KF by ciphering title deed data 106 and content key data Kc that a content provider 101 generates with key data for distribution and sends the file to a content provider 101. The content provider 101 supply a secure container 104 including a content file CF containing the content data C deciphered by using the content key data Kc and the key file KF received from the EMD service center 102 to SAM 105, etc., of a user home network 103.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－94549
（P2001－94549A）
(43)公開日　平成13年４月６日(2001.4.6)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)
Ｈ０４Ｌ	9/08		Ｇ０６Ｆ	12/14	３２０Ｂ　５Ｂ０１７
Ｇ０６Ｆ	12/14	３２０		15/00	３３０Ｚ　５Ｂ０８５
	15/00	３３０	Ｇ０９Ｃ	1/00	６４０Ｂ　５Ｄ０４４
Ｇ０９Ｃ	1/00	６４０			６４０Ｚ　５Ｊ１０４
					６６０Ｄ　９Ａ００１

審査請求　未請求　請求項の数103　書面　（全253頁）　最終頁に続く

(21)出願番号　特願平11－309721

(22)出願日　平成11年９月17日(1999.9.17)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

(72)発明者　野中　聡
東京都品川区北品川６丁目７番35号　ソニー株式会社内

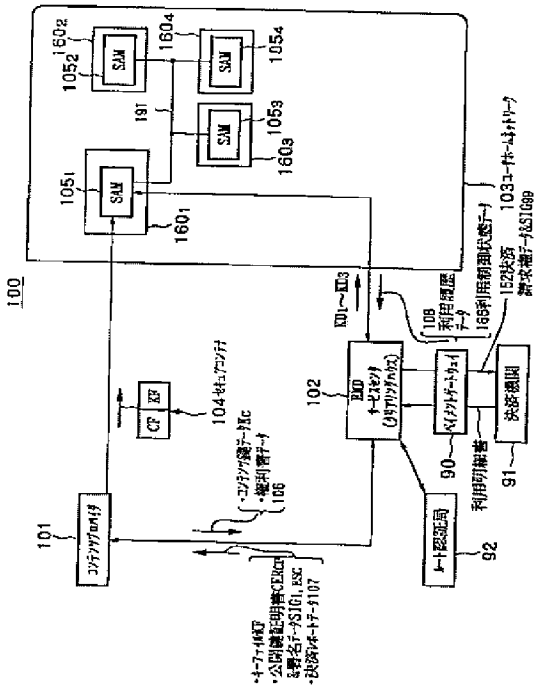
(72)発明者　江崎　正
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(74)代理人　100094053
弁理士　佐藤　隆久

最終頁に続く

(54)【発明の名称】　データ提供システムおよびその方法

(57)【要約】
【課題】　データ提供装置の関係者の利益を保護できるデータ提供システムを提供する。
【解決手段】　ＥＭＤサービスセンタ１０２はコンテンツプロバイダ１０１が作成した権利書データ１０６およびコンテンツ鍵データＫｃを配信用鍵データで暗号して格納したキーファイルＫＦを作成し、これをコンテンツプロバイダ１０１に送る。コンテンツプロバイダ１０１は、コンテンツ鍵データＫｃを用いて暗号されたコンテンツデータＣを含むコンテンツファイルＣＦと、ＥＭＤサービスセンタ１０２から受けたキーファイルＫＦとを含むセキュアコンテナ１０４をユーザホームネットワーク１０３のＳＡＭ１０５ｉなどに配給する。



1

【特許請求の範囲】

【請求項１】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化された前記コンテンツデータを提供し、

前記データ処理装置は、前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定するデータ提供システム。

【請求項２】前記管理装置は、前記キーファイルの作成者の正当性を検証するための署名データを前記キーファイルに付加する請求項１に記載のデータ提供システム。

【請求項３】前記データ提供装置は、前記コンテンツデータを格納したコンテンツファイルを作成し、当該コンテンツファイルを前記データ処理装置に提供する請求項１に記載のデータ提供システム。

【請求項４】前記データ提供装置は、前記コンテンツファイルの作成者の正当性を検証するための署名データを前記コンテンツファイルに付加する請求項３に記載のデータ提供システム。

【請求項５】前記データ提供装置は、前記権利書データを作成して前記管理装置に送り、

前記データ処理装置は、前記権利書データに基づいて、前記配給を受けたコンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置は、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置の関係者に分配するための利益分配処理を行う請求項１に記載のデータ提供システム。

【請求項６】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納したモジュールを、前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定するデータ提供システム。

2

【請求項７】前記管理装置は、前記キーファイルの作成者の正当性を検証するための署名データを生成し、当該署名データをさらに格納した前記キーファイルを作成する請求項６に記載のデータ提供システム。

【請求項８】前記データ提供装置は、前記コンテンツ鍵データおよび前記権利書データを生成して前記管理装置に送信し、

前記管理装置は、受信した前記コンテンツ鍵データおよび前記権利書データに基づいて前記キーファイルを作成し、当該作成したキーファイルを登録する請求項６に記載のデータ提供システム。

【請求項９】前記データ提供装置は、前記コンテンツファイルの作成者および配給者と、前記キーファイルの配給者との正当性のうち少なくとも一つを検証するための署名データをそれぞれ作成し、当該署名データをさらに格納した前記モジュールを前記データ処理装置に配給する請求項７に記載のデータ提供システム。

【請求項１０】前記データ処理装置は、前記モジュールに格納された前記署名データを検証して、前記コンテンツファイルの作成者および配給者と、前記キーファイルの作成者および配給者との正当性のうち少なくとも一つを確認する請求項９に記載のデータ提供システム。

【請求項１１】前記管理装置は、配信用鍵データを用いて暗号化した前記コンテンツ鍵データおよび前記権利書データを格納した前記キーファイルを作成し、

前記配信用鍵データを前記データ処理装置に配給する請求項６に記載のデータ提供システム。

【請求項１２】前記管理装置および前記データ処理装置は、有効期間が規定された複数の配信用鍵データを有し、対応する期間の前記配信用鍵データを用いる請求項１１に記載のデータ提供システム。

【請求項１３】前記データ提供装置は、自らの秘密鍵データを用いて前記署名データを作成し、

前記データ処理装置は、前記秘密鍵データに対応する公開鍵データを用いて、前記署名データの正当性を検証する請求項１０に記載のデータ提供システム。

【請求項１４】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納

3

したモジュールを、前記データ処理装置に配給し、
前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定するデータ提供システム。

【請求項１５】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、
前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、
前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを個別に前記データ処理装置に配給し、
前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項１６】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、
前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、
前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを前記データ処理装置に配給し、
前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項１７】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、
前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、
前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納したモジュールを前記

4

データ処理装置に配給し、
前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定するデータ提供システム。

【請求項１８】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、
前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、
前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを個別に前記データ処理装置に配給し、
前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項１９】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、
前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、
前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ処理装置に配給し、
前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定するデータ提供システム。

【請求項２０】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、
前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成し、
前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ処理装置に配給し、

5

前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項２１】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成して前記データ処理装置に配給し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定するデータ提供システム。

【請求項２２】データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化された前記コンテンツデータを提供し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項２３】前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第１のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記第１のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第２のモジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記第２のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する請求項２２に記載のデータ提供システム。

【請求項２４】前記データ配給装置は、前記提供を受けた第１のモジュールを包括させた前記第２のモジュールを作成し、当該作成した第２のモジュールを前記データ処理装置に配給する請求項２２に記載のデータ提供システム。

【請求項２５】前記データ配給装置は、前記コンテンツデータの価格を示す価格データをさらに格納した前記第２のモジュールを前記データ処理装置に配給する請求項２２に記載のデータ提供システム。

【請求項２６】前記データ配給装置は、前記データ提供装置が前記コンテンツデータについて決定した卸売価格に基づいて、前記価格データを決定する請求項２５に記載のデータ提供システム。

【請求項２７】前記データ提供装置は、

前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データのうち少なくとも一つのデータの作成者および送信者の正当性を検証するための署名データをさらに格納した前記第１のモジュールを前記データ配給装置に提供する請求項２２に記載のデータ提供システム。

【請求項２８】前記データ配給装置は、

前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データのうち少なくとも一つのデータの作成者および送信者の正当性を検証するための署名データをさらに格納した前記第２のモジュールを前記データ処理装置に提供する請求項２２に記載のデータ提供システム。

【請求項２９】前記データ処理装置は、前記権利書データに基づいて、前記配給を受けたコンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置は、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う請求項２２に記載のデータ提供システム。

【請求項３０】前記データ処理装置は、前記データ配給装置の前記配給に関しての配給用履歴データを前記データ配給装置に送信し、

前記データ配給装置は、前記配給用履歴データに基づいて、前記配給に関しての課金処理を行う請求項２２に記載のデータ提供システム。

【請求項３１】データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前

7

記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、
前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納した第１のモジュールを前記データ配給装置に提供し、
前記データ配給装置は、前記提供を受けたコンテンツファイルおよび前記キーファイルを格納した第２のモジュールを前記データ処理装置に配給し、
前記データ処理装置は、前記配給を受けた前記第２のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第２のモジュールに格納された前記コンテンツデータの取り扱いを決定するデータ提供システム。
【請求項３２】前記データ提供装置は、前記コンテンツ鍵データおよび前記権利書データを生成して前記管理装置に送信し、
前記管理装置は、受信した前記コンテンツ鍵データおよび前記権利書データに基づいて前記キーファイルを作成し、前記受信した前記コンテンツ鍵データおよび前記権利書データを登録する請求項３１に記載のデータ提供システム。
【請求項３３】前記データ提供装置は、前記コンテンツファイルの作成者および提供者と、前記キーファイルの提供者との正当性のうち少なくとも一つを検証するための署名データをそれぞれ作成し、当該署名データをさらに格納した前記第１のモジュールを前記データ処理装置に配給する請求項３１に記載のデータ提供システム。
【請求項３４】前記データ配給装置は、前記コンテンツファイルの作成者および配給者と、前記キーファイルの配給者との正当性のうち少なくとも一つを検証するための署名データをそれぞれ作成し、当該署名データをさらに格納した前記第２のモジュールを前記データ処理装置に配給する請求項３１に記載のデータ提供システム。
【請求項３５】前記データ提供装置は、自らの秘密鍵データを用いて前記署名データを作成し、
前記データ処理装置は、前記秘密鍵データに対応する公開鍵データを用いて、前記署名データの正当性を検証する請求項３３に記載のデータ提供システム。
【請求項３６】前記データ提供装置は、前記公開鍵データの正当性を証明する公開鍵証明書データをさらに格納した前記モジュールを前記データ処理装置に配給し、
前記データ処理装置は、前記配給を受けた公開鍵証明書データに格納された公開鍵データを用いて前記署名データの検証を行う請求項３３に記載のデータ提供システム。
【請求項３７】前記管理装置は、前記公開鍵データの正当性を証明する公開鍵証明書データを前記データ処理装

8

置に配給する前記データ処理装置は、前記配給を受けた公開鍵証明書データに格納された公開鍵データを用いて前記署名データの検証を行う請求項３６に記載のデータ提供システム。
【請求項３８】前記データ配給装置は、自らの秘密鍵データを用いて前記署名データを作成し、
前記データ処理装置は、前記秘密鍵データに対応する公開鍵データを用いて、前記署名データの正当性を検証する請求項３３に記載のデータ提供システム。
【請求項３９】前記データ配給装置は、前記公開鍵データの正当性を証明する公開鍵証明書データをさらに格納した前記モジュールを前記データ処理装置に配給し、
前記データ処理装置は、前記配給を受けた公開鍵証明書データに格納された公開鍵データを用いて前記署名データの検証を行う請求項３８に記載のデータ提供システム。
【請求項４０】前記管理装置は、前記公開鍵データの正当性を証明する公開鍵証明書データを前記データ処理装置に配給する前記データ処理装置は、前記配給を受けた公開鍵証明書データに格納された公開鍵データを用いて前記署名データの検証を行う請求項３８に記載のデータ提供システム。
【請求項４１】前記データ処理装置は、前記権利書データに基づいて、前記配給を受けたコンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、
前記管理装置は、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う請求項３１に記載のデータ提供システム。
【請求項４２】前記データ配給装置は、前記コンテンツデータの価格を示す価格データを格納した前記第２のモジュールを前記データ処理装置に配給する請求項３１に記載のデータ提供システム。
【請求項４３】前記管理装置は、前記データ配給装置から受けた前記価格データを登録する請求項４２に記載のデータ提供システム。
【請求項４４】前記データ処理装置は、その処理内容、内部メモリに記憶された所定のデータおよび処理中のデータを、外部から監視および改竄困難なモジュールを有する請求項３１に記載のデータ提供システム。
【請求項４５】データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、
前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納した第１のモジュールを前記データ配給装置に提供し、
前記データ配給装置は、前記提供を受けたコンテンツファイルを格納した第２のモジュールを前記データ処理装置に配給し、
前記データ処理装置は、前記配給を受けた前記第２のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第２のモジュールに格納された前記コンテンツデータの取り扱いを決定するデータ提供システム。
【請求項４６】データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、
前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、
前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを個別に前記データ配給装置に配給し、
前記データ配給装置は、配給を受けた前記コンテンツファイルと前記キーファイルとを個別に前記データ処理装置に配給し、
前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供システム。
【請求項４７】前記コンテンツファイルおよび前記キーファイルには、相互の対応関係を明示するためのデータが含まれる請求項４６に記載のデータ提供システム。
【請求項４８】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、
前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、
前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを前記データ配給装置に提供し、
前記データ配給装置は、前記提供を受けたコンテンツファイルを前記データ処理装置に配給し、
前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供システム。
【請求項４９】前記コンテンツファイルおよび前記キーファイルには、相互の対応関係を明示するためのデータが含まれる請求項４８に記載のデータ提供システム。
【請求項５０】データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、
前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、
前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納した第１のモジュールを前記データ配給装置に提供し、
前記データ配給装置は、前記提供を受けたコンテンツデータおよび前記キーファイルを格納した第２のモジュールを前記データ処理装置に配給し、
前記データ処理装置は、前記配給を受けた前記第２のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第２のモジュールに格納された前記コンテンツデータの取り扱いを決定するデータ提供システム。
【請求項５１】データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、
前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、
前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを個別に前記データ配給装置に配給し、
前記データ配給装置は、配給を受けた前記コンテンツデータと前記キーファイルとを個別に前記データ配給装置

に配給し、
前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定するデータ提供システム。
【請求項５２】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、
前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、
前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、
前記データ配給装置は、前記提供を受けたコンテンツデータを前記データ処理装置に配給し、
前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定するデータ提供システム。
【請求項５３】データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、
前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ提供装置に提供し、
前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ配給装置に配給し、
前記データ配給装置は、配給を受けた前記コンテンツデータと前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ配給装置に配給し、
前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定するデータ提供システム。
【請求項５４】データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムにおいて、
前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ処理装置に配給し、
前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、
前記データ配給装置は、前記提供を受けたコンテンツデータを前記データ処理装置に配給し、
前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定するデータ提供システム。
【請求項５５】データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムにおいて、
前記データ提供装置は、コンテンツのマスタソースデータを前記管理装置に提供し、
前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスタソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルおよび前記キーファイルを前記データ配給装置に提供し、
前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを前記データ処理装置に配給し、
前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供システム。
【請求項５６】前記管理装置は、前記コンテンツファイルおよび前記キーファイルを格納した第１のモジュールを作成し、当該第１のモジュールを前記データ配給装置に提供し、
前記データ配給装置は、前記第１のモジュールに格納された前記コンテンツファイルおよび前記キーファイルを格納した第２のモジュールを生成し、当該第２のモジュールを前記データ処理装置に配給する請求項５５に記載のデータ提供システム。
【請求項５７】前記管理装置は、前記コンテンツファイルを記憶および管理するデータベース、前記キーファイルを記憶および管理するデータベース、および前記権利

書データを記憶および管理するデータベースのうち、少なくとも一つのデータベースを有し、
前記コンテンツデータに固有に割り当てられたコンテンツ識別子を用いて、前記コンテンツファイル、前記キーファイルおよび前記権利書データの少なくとも一つを一元的に管理する請求項５５に記載のデータ提供システム。

【請求項５８】データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムにおいて、
前記データ提供装置は、コンテンツのマスタソースデータを前記管理装置に提供し、
前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスタソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルを前記データ配給装置に提供し、前記キーファイルを前記データ処理装置に提供し、
前記データ配給装置は、前記提供を受けた前記コンテンツファイルを前記データ処理装置に配給し、
前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項５９】データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムにおいて、
前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、
前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルと、前記作成したキーファイルとを前記データ配給装置に提供し、
前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを前記データ処理装置に配給し、
前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項６０】前記管理装置は、前記コンテンツファイルおよび前記キーファイルを格納した第１のモジュールを作成し、当該第１のモジュールを前記データ配給装置に提供し、
前記データ配給装置は、前記第１のモジュールに格納された前記コンテンツファイルおよび前記キーファイルを格納した第２のモジュールを生成し、当該第２のモジュールを前記データ処理装置に配給する請求項５９に記載のデータ提供システム。

【請求項６１】データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムにおいて、
前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、
前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルを前記データ配給装置に提供し、前記作成したキーファイルを前記データ処理装置に提供し、
前記データ配給装置は、前記提供を受けた前記コンテンツファイルを前記データ処理装置に配給し、
前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項６２】データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、
前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、
前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ提供装置に提供し、
前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項６３】データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、

前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記データ配給装置から提供を受けたキーファイルとを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項６４】データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、

前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項６５】複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび対応する前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、

前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを対応する前記データ提供装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項６６】複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、

前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、

前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項６７】複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処

理装置を有するデータ提供システムにおいて、
前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、
前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、
前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを前記データ処理装置に配給し、
前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項６８】複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、
前記データ提供装置は、コンテンツデータのマスタソースを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルおよびキーファイルを前記データベースに格納し、
前記管理装置は、対応する前記データ提供装置から受けた前記マスタソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記作成したコンテンツファイルおよび前記作成したキーファイルを対応する前記データ提供装置に送り、
前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを前記データ処理装置に配給し、
前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項６９】複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツデータのマスタソースを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記データベースに格納し、
前記管理装置は、対応する前記データ提供装置から受けた前記マスタソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを対応する前記データ配給装置に送り、
前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを前記データ処理装置に配給し、
前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項７０】複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムにおいて、
前記データ提供装置は、コンテンツデータのマスタソースを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記データベースに格納し、
前記管理装置は、対応する前記データ提供装置から受けた前記マスタソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、
前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを前記データ処理装置に配給し、
前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供システム。

【請求項７１】データ提供装置からデータ処理装置にコ

ンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化された前記コンテンツデータを提供し、

前記データ処理装置は、前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定するデータ提供方法。

【請求項７２】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記作成したキーファイルを前記管理装置から前記データ提供装置に配給し、

前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から配給を受けた前記キーファイルとを格納したモジュールを前記データ提供装置から前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定するデータ提供方法。

【請求項７３】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納したモジュールを前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定するデータ提供方法。

【請求項７４】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

当該作成したキーファイルを前記管理装置から前記データ提供装置に配給し、

前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを個別に前記データ提供装置から前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供方法。

【請求項７５】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

当該作成したキーファイルを前記管理装置から前記データ処理装置に配給し、

前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを前記データ提供装置から前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供方法。

【請求項７６】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納したモジュールを前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定するデータ提供方法。

21

【請求項７７】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを個別に前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定するデータ提供方法。

【請求項７８】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定するデータ提供方法。

【請求項７９】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供方法。

22

【請求項８０】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成して前記データ処理装置に配給し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定するデータ提供方法。

【請求項８１】データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記コンテンツ鍵データを用いて暗号化された前記コンテンツデータを前記データ提供装置から前記データ配給装置に提供し、

前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置は、前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定するデータ提供方法。

【請求項８２】データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

当該作成したキーファイルを前記管理装置から前記データ提供装置に配給し、

前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納した第１のモジュールを、前記データ提供装置から前記データ配給装置に提供し、

前記提供を受けたコンテンツファイルおよび前記キーファイルを格納した第２のモジュールを前記データ配給装置から前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記第２のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第２のモジュールに格納された前記コンテンツデータの取り扱いを決定するデータ提供方法。

【請求項８３】データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納した第１のモジュールを前記データ配給装置に提供し、

前記データ配給装置において、前記提供を受けたコンテンツファイルを格納した第２のモジュールを前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記第２のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第２のモジュールに格納された前記コンテンツデータの取り扱いを決定するデータ提供方法。

【請求項８４】データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記作成したキーファイルを前記管理装置から前記データ提供装置に配給し、

前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを個別に前記データ提供装置から前記データ配給装置に配給し、

前記配給を受けた前記コンテンツファイルと前記キーファイルとを個別に前記データ配給装置から前記データ配給装置に配給し、

前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ

提供方法。

【請求項８５】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

当該作成したキーファイルを前記管理装置から前記データ処理装置に配給し、

前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを前記データ提供装置から前記データ配給装置に提供し、

前記提供を受けたコンテンツファイルを前記データ配給装置から前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供方法。

【請求項８６】データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納した第１のモジュールを前記データ配給装置に提供し、

前記データ配給装置において、前記提供を受けたコンテンツデータおよび前記キーファイルを格納した第２のモジュールを前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記第２のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第２のモジュールに格納された前記コンテンツデータの取り扱いを決定するデータ提供方法。

【請求項８７】データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを個別に前記データ配給装置に配給し、

前記データ配給装置において、配給を受けた前記コンテンツデータと前記キーファイルとを個別に前記データ配給装置に配給し、

前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定するデータ提供方法。

【請求項８８】データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、

前記データ配給装置において、前記提供を受けたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定するデータ提供方法。

【請求項８９】データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ提供装置に提供し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ配給装置に配給し、

前記データ配給装置において、配給を受けた前記コンテンツデータと前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ配給装置に配給し、

前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当

該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定するデータ提供方法。

【請求項９０】データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法において、

前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ処理装置に配給し、

前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けたコンテンツデータを前記データ処理装置に配給し、

前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定するデータ提供方法。

【請求項９１】データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツのマスタソースデータを前記管理装置に提供し、

前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスタソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルおよび前記キーファイルを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供方法。

【請求項９２】データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置は、コンテンツのマスタソースデータを前記管理装置に提供し、

前記管理装置は、前記データ提供装置、前記データ

装置および前記データ処理装置を管理し、前記提供されたマスタソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルを前記データ配給装置に提供し、前記キーファイルを前記データ処理装置に提供し、
前記データ配給装置は、前記提供を受けた前記コンテンツファイルを前記データ処理装置に配給し、
前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供方法。

【請求項９３】データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法において、
前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、
前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルと、前記作成したキーファイルとを前記データ配給装置に提供し、
前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを前記データ処理装置に配給し、
前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供方法。

【請求項９４】データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法において、
前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、
前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルを前記データ配給装置に提供し、前記作成したキーファイルを前記データ処理装置に提供し、
前記データ配給装置は、前記提供を受けた前記コンテンツファイルを前記データ処理装置に配給し、
前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供方法。

【請求項９５】データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、
前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、
前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ提供装置に提供し、
前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを前記データ処理装置に配給し、
前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供方法。

【請求項９６】データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、
前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、
前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、
前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記データ配給装置から提供を受けたキーファイルとを前記データ処理装置に配給

し、
前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供方法。
【請求項９７】データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、
前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、
前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、
前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを前記データ処理装置に配給し、
前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供方法。
【請求項９８】複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、
前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび対応する前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、
前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを対応する前記データ提供装置に提供し、
前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを前記データ処理装置に配給し、
前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供方法。
【請求項９９】複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、
前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、
前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、
前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを前記データ処理装置に配給し、
前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供方法。
【請求項１００】複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、
前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、
前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、
前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを前記データ処理装置に配給し、
前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供方法。
【請求項１０１】複数のデータ提供装置、データ配給装

置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、
前記データ提供装置は、コンテンツデータのマスタソースを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルおよびキーファイルを前記データベースに格納し、
前記管理装置は、対応する前記データ提供装置から受けた前記マスタソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記作成したコンテンツファイルおよび前記作成したキーファイルを対応する前記データ提供装置に送り、
前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを前記データ処理装置に配給し、
前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供方法。
【請求項１０２】複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、
前記データ提供装置は、コンテンツデータのマスタソースを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記データベースに格納し、
前記管理装置は、対応する前記データ提供装置から受けた前記マスタソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを対応する前記データ配給装置に送り、
前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを前記データ処理装置に配給し、
前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供方法。
【請求項１０３】複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法において、
前記データ提供装置は、コンテンツデータのマスタソースを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記データベースに格納し、
前記管理装置は、対応する前記データ提供装置から受けた前記マスタソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、
前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを前記データ処理装置に配給し、
前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定するデータ提供方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、コンテンツデータを提供するデータ提供システムおよびその方法に関する。
【０００２】
【従来の技術】暗号化されたコンテンツデータを所定の契約を交わしたユーザのデータ処理装置に配給し、当該データ処理装置において、コンテンツデータを復号して再生および記録するデータ提供システムがある。このようなデータ提供システムの一つに、音楽データを配信する従来のＥＭＤ（Ｅｌｅｃｔｒｏｎｉｃ　Ｍｕｓｉｃ　Ｄｉｓｔｒｉｂｕｔｉｏｎ：電子音楽配信）システムがある。
【０００３】図１４５は、従来のＥＭＤシステム７００の構成図である。図１４５に示すＥＭＤシステム７００では、コンテンツプロバイダ７０１ａ，７０１ｂが、サービスプロバイダ７１０に対し、コンテンツデータ７０４ａ，７０４ｂ，７０４ｃと、著作権情報７０５ａ，７０５ｂ，７０５ｃとを、それぞれ相互認証後に得たセッション鍵データで暗号化してオンラインで供給したり、あるいはオフラインで供給する。ここで、著作権情報７０５ａ，７０５ｂ，７０５ｃには、例えば、ＳＣＭＳ

33

（Ｓｅｒｉａｌ　Ｃｏｐｙ　ＭａｎａｇｅｍｅｎｔＳｙｓｔｅｍ）情報、コンテンツデータに埋め込むことを要請する電子透かし情報およびサービスプロバイダ７１０の伝送プロトコルに埋め込むことを要請する著作権に関する情報などがある。

【０００４】サービスプロバイダ７１０は、受信したコンテンツデータ７０４ａ，７０４ｂ，７０４ｃと、著作権情報７０５ａ，７０５ｂ，７０５ｃとをセッション鍵データを用いて復号する。そして、サービスプロバイダ７１０は、復号したあるいはオフラインで受け取ったコンテンツデータ７０４ａ，７０４ｂ，７０４ｃに、著作権情報７０５ａ，７０５ｂ，７０５ｃを埋め込んで、コンテンツデータ７０７ａ，７０７ｂ，７０７ｃを生成する。このとき、サービスプロバイダ７１０は、例えば、著作権情報７０５ａ，７０５ｂ，７０５ｃのうち電子透かし情報をコンテンツデータ７０４ａ，７０４ｂ，７０４ｃに所定の周波数領域を変更して埋め込み、当該コンテンツデータをユーザに送信する際に用いるネットワークプロトコルにＳＣＭＳ情報を埋め込む。さらに、サービスプロバイダ７１０は、コンテンツデータ７０７ａ，７０７ｂ，７０７ｃを、鍵データベース７０６から読み出したコンテンツ鍵データＫｃａ，Ｋｃｂ，Ｋｃｃを用いてそれぞれ暗号化する。その後、サービスプロバイダ７１０は、暗号化されたコンテンツデータ７０７ａ，７０７ｂ，７０７ｃを格納したセキュアコンテナ７２２を、相互認証後に得たセッション鍵データによって暗号化してユーザの端末装置７０９に存在するＣＡ（Ｃｏｎｄｉｔｉｏｎａｌ　Ａｃｃｅｓｓ）モジュール７１１に送信する。

【０００５】ＣＡモジュール７１１は、セキュアコンテナ７２２をセッション鍵データを用いて復号する。また、ＣＡモジュール７１１は、電子決済やＣＡなどの課金機能を用いて、サービスプロバイダ７１０の鍵データベース７０６からコンテンツ鍵データＫｃａ，Ｋｃｂ，Ｋｃｃを受信し、これをセッション鍵データを用いて復号する。これにより、端末装置７０９において、コンテンツデータ７０７ａ，７０７ｂ，７０７ｃを、それぞれコンテンツ鍵データＫｃａ，Ｋｃｂ，Ｋｃｃを用いて復号することが可能になる。このとき、ＣＡモジュール７１１は、コンテンツ単位で課金処理を行い、その結果に応じた課金情報７２１を生成し、これをセッション鍵データで暗号化した後に、サービスプロバイダ７１０の権利処理モジュール７２０に送信する。この場合に、ＣＡモジュール７１１は、サービスプロバイダ７１０が自らの提供するサービスに関して管理したい項目であるユーザの契約（更新）情報および月々基本料金などのネットワーク家賃の徴収と、コンテンツ単位の課金処理と、ネットワークの物理層のセキュリティー確保とを行う。

【０００６】サービスプロバイダ７１０は、ＣＡモジュール７１１から課金情報７２１を受信すると、サービス

34

プロバイダ７１０とコンテンツプロバイダ７０１ａ，７０１ｂ，７０１ｃとの間で利益配分を行う。このとき、サービスプロバイダ７１０から、コンテンツプロバイダ７０１ａ，７０１ｂ，７０１ｃへの利益配分は、例えば、ＪＡＳＲＡＣ（ＪａｐａｎｅｓｅＳｏｃｉｅｔｙ　ｆｏｒ　Ｒｉｇｈｔｓ　ｏｆ　Ａｕｔｈｏｒｓ，Ｃｏｍｐｏｓｅｒｓ　ａｎｄ　Ｐｕｂｌｉｓｈｅｒｓ：日本音楽著作権協会）を介して行われる。また、ＪＡＳＲＡＣによって、コンテンツプロバイダの利益が、当該コンテンツデータの著作権者、アーティスト、作詞・作曲家および所属プロダクションなどに分配される。

【０００７】また、端末装置７０９では、コンテンツ鍵データＫｃａ，Ｋｃｂ，Ｋｃｃを用いて復号したコンテンツデータ７０７ａ，７０７ｂ，７０７ｃを、ＲＡＭ型の記録媒体７２３などに記録する際に、著作権情報７０５ａ，７０５ｂ，７０５ｃのＳＣＭＳビットを書き換えて、コピー制御を行う。すなわち、ユーザ側では、コンテンツデータ７０７ａ，７０７ｂ，７０７ｃに埋め込まれたＳＣＭＳビットに基づいて、コピー制御が行われ、著作権の保護が図られている。

【０００８】

【発明が解決しようとする課題】ところで、ＳＣＭＳは、コンテンツデータを例えば２世代以上のわたって複製することを禁止するものであり、１世代の複製は無限に行うことができ、著作権者の保護として不十分であるという問題がある。

【０００９】また、上述したＥＭＤシステム７００では、サービスプロバイダ７１０が暗号化されていないコンテンツデータを技術的には自由に扱えるため、コンテンツプロバイダ７０１の関係者はサービスプロバイダ７１０の行為等を監視する必要があり、当該監視の負担が大きいと共に、コンテンツプロバイダ７０１の利益が不当に損なわれる可能性が高いという問題がある。また、上述したＥＭＤシステム７００では、ユーザの端末装置７０９がサービスプロバイダ７１０から配給を受けたコンテンツデータをオーサリングして他の端末装置などに再配給する行為を規制することが困難であり、コンテンツプロバイダ７０１の利益が不当に損なわれるという問題がある。

【００１０】本発明は上述した従来技術の問題点に鑑みてなされ、コンテンプロバイダの権利者（関係者）の利益を適切に保護できるデータ提供システムおよびその方法を提供することを目的とする。また、本発明は、コンテンプロバイダの権利者の利益を保護するための監査の負担を軽減できるデータ提供システムおよびその方法を提供することを目的とする。

【００１１】

【課題を解決するための手段】上述した従来技術の問題点を解決し、上述した目的を達成するために、本発明の第１の観点のデータ提供システムは、好ましくは、デー

タ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化された前記コンテンツデータを提供し、前記データ処理装置は、前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【００１２】本発明の第１の観点のデータ提供システムの作用は以下に示すようになる。前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該キーファイルが前記データ提供装置に送られる。そして、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化された前記コンテンツデータが提供される。そして、前記データ処理装置において、前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いが決定される。

【００１３】また、本発明の第２の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納したモジュールを、前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【００１４】本発明の第２の観点のデータ提供システムの作用は以下に示すようになる。管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成される。そして、当該作成されたキーファイルが、前記管理装置から前記データ提供装置に配給される。そして、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイル

とを格納したモジュールが、前記データ提供装置から前記データ処理装置に配給される。そして、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号された権利書データに基づいて、前記コンテンツデータの取り扱いが決定される。

【００１５】本発明の第３の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納したモジュールを、前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【００１６】本発明の第３の観点のデータ提供システムの作用は以下に示すようになる。前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該キーファイルが前記データ提供装置に送られる。そして、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納したモジュールが配給される。そして、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号され権利書データに基づいて、前記コンテンツデータの取り扱いが決定される。

【００１７】また、本発明の第４の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、　前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを個別に前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づい

て、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【００１８】本発明の第４の観点のデータ提供システムの作用は以下に示すようになる。前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該キーファイルが前記データ提供装置に送られる。そして、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとが配給される。そして、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号された権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いが決定される。

【００１９】また、本発明の第５の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【００２０】本発明の第５の観点のデータ提供システムの作用は以下に示すようになる。前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成される。当該作成されたキーファイルは、前記管理装置から前記データ処理装置に配給される。また、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルが配給される。そして、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いが決定される。

【００２１】また、本発明の第６の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納したモジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【００２２】本発明の第６の観点のデータ提供システムの作用は以下に示すようになる。前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該キーファイルが前記データ提供装置に送られる。そして、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納したモジュールが配給される。そして、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データが復号し、当該復号しされた権利書データに基づいて、前記コンテンツデータの取り扱いが決定される。

【００２３】また、本発明の第７の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを個別に前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

【００２４】本発明の第７の観点のデータ提供システムの作用は以下に示すようになる。前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該キーファイルが前記データ提供装置に送られる。そして、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管

39

理装置から受けた前記キーファイルとが個別に配給される。そして、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号された権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いが決定される。

【００２５】また、本発明の第８の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

【００２６】本発明の第８の観点のデータ提供システムの作用は以下に示すようになる。前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該作成されたキーファイルが前記データ処理装置に配給される。また、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータが配給される。そして、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号された権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いが決定される。

【００２７】また、本発明の第９の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

40

【００２８】本発明の第９の観点のデータ提供システムの作用は以下に示すようになる。前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとが作成され、これらが前記データ提供装置に送られる。そして、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとが個別に配給される。そして、前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号された権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いが決定される。

【００２９】また、本発明の第１０の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成して前記データ処理装置に配給し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

【００３０】本発明の第１０の観点のデータ提供システムの作用は以下に示すようになる。前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとが作成され、これらが前記データ処理装置に配給される。また、前記データ提供装置から前記データ処理装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータが配給される。そして、前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いが決定される。

【００３１】また、本発明の第１１の観点のデータ提供システムは、データ提供装置、データ配給装置、データ処理装置および管理装置を有するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化された前記コンテンツデータを提供し、前記データ配給装置は、前記提供されたコンテンツデータを前

記データ処理装置に配給し、前記データ処理装置は、前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

【００３２】本発明の第の１１観点のデータ提供システムの作用は以下に示すようになる。前記管理装置において、、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成される。そして、前記データ提供装置から前記データ配給装置に、前記コンテンツ鍵データを用いて暗号化された前記コンテンツデータが提供される。そして、前記データ配給装置から前記データ処理装置に、前記提供されたコンテンツデータが配給される。そして、前記データ処理装置において、前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号された権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いが決定される。

【００３３】また、本発明の第１２の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納した第１のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けたコンテンツファイルおよび前記キーファイルを格納した第２のモジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第２のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第２のモジュールに格納された前記コンテンツデータの取り扱いを決定する。

【００３４】本発明の第１２の観点のデータ提供システムの作用は以下に示すようになる。前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルが作成され、当該キーファイルが前記データ提供装置に送られる。そして、前記データ提供装置から前記データ配給装置に、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納した第１のモジュールが提供される。そして、前記データ配給装置から前記データ処理装置に、前記提供を受けたコンテンツファイルおよび前記キーファイルを格納した第２のモジュールが配給される。そして、前記データ処理装置において、前記配給を受けた前記第２のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号された権利書データに基づいて、前記配給を受けた前記第２のモジュールに格納された前記コンテンツデータの取り扱いが決定される。

【００３５】また、本発明の第１３の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納した第１のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けたコンテンツファイルを格納した第２のモジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第２のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第２のモジュールに格納された前記コンテンツデータの取り扱いを決定する。

【００３６】また、本発明の第１４の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを個別に前記データ配給装置に配給し、前記データ配給装置は、配給を受けた前記コンテンツファイルと前記キーファイルとを個別に前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

43

【００３７】また、本発明の第１５の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けたコンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【００３８】また、本発明の第１６の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納した第１のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けたコンテンツデータおよび前記キーファイルを格納した第２のモジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第２のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第２のモジュールに格納された前記コンテンツデータの取り扱いを決定する。

【００３９】また、本発明の第１７の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを個別に前記データ配給装置に配給し、前記データ配給装置は、配給を受けた前記コンテンツデータと前記キーファイルとを個別に前記データ配給装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

44

【００４０】また、本発明の第１８の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

【００４１】また、本発明の第１９の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ提供装置に提供し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ配給装置に配給し、前記データ配給装置は、配給を受けた前記コンテンツデータと前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ配給装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

【００４２】また、本発明の第２０の観点のデータ提供システムは、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記

データ処理装置を管理するデータ提供システムであって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ処理装置に配給し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

【００４３】また、本発明の第２１の観点のデータ提供システムは、データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツのマスタソースデータを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスタソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルおよび前記キーファイルを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【００４４】また、本発明の第２２の観点のデータ提供システムは、データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツのマスタソースデータを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスタソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルを前記データ配給装置に提供し、前記キーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【００４５】また、本発明の第２３の観点のデータ提供システムは、データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルと、前記作成したキーファイルとを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【００４６】また、本発明の第２４の観点のデータ提供システムは、データ提供装置、データ配給装置、管理装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルを前記データ配給装置に提供し、前記作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【００４７】また、本発明の第２５の観点のデータ提供システムは、データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテ

ンツファイルを作成し、当該作成したコンテンツファイルおよび前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ提供装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【００４８】また、本発明の第２６の観点のデータ提供システムは、データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記データ配給装置から提供を受けたキーファイルとを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【００４９】また、本発明の第２７の観点のデータ提供システムは、データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを

復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【００５０】また、本発明の第２８の観点のデータ提供システムは、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび対応する前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを対応する前記データ提供装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【００５１】また、本発明の第２９の観点のデータ提供システムは、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【００５２】また、本発明の第３０の観点のデータ提供システムは、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提

供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【００５３】また、本発明の第３１の観点のデータ提供システムは、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータのマスタソースを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルおよびキーファイルを前記データベースに格納し、前記管理装置は、対応する前記データ提供装置から受けた前記マスタソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記作成したコンテンツファイルおよび前記作成したキーファイルを対応する前記データ提供装置に送り、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【００５４】また、本発明の第３２の観点のデータ提供システムは、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータのマスタソースを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記データベースに格納し、前記管理装置は、対応する前記データ提供装置から受けた前記マスタソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを対応する前記データ配給装置に送り、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【００５５】また、本発明の第３３の観点のデータ提供システムは、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツデータのマスタソースを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記データベースに格納し、前記管理装置は、対応する前記データ提供装置から受けた前記マスタソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【００５６】また、本発明の第１の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化された前記コンテンツデータを提供し、前記データ処理装置は、前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当

該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【００５７】また、本発明の第２の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記作成したキーファイルを前記管理装置から前記データ提供装置に配給し、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から配給を受けた前記キーファイルとを格納したモジュールを前記データ提供装置から前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【００５８】また、本発明の第３の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納したモジュールを前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【００５９】また、本発明の第４の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記管理装置から前記データ提供装置に配給し、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを個別に前記データ提供装置から前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号し

た権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【００６０】また、本発明の第５の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記管理装置から前記データ処理装置に配給し、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを前記データ提供装置から前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【００６１】また、本発明の第６の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納したモジュールを前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【００６２】また、本発明の第７の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを個別に前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

53

【００６３】また、本発明の第８の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

【００６４】また、本発明の第９の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【００６５】また、本発明の第１０の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを作成して前記データ処理装置に配給し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

【００６６】また、本発明の第１１の観点のデータ提供方法は、データ提供装置、データ配給装置、データ処理装置および管理装置を用いたデータ提供システムであって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化

54

された権利書データとを格納したキーファイルを作成し、前記コンテンツ鍵データを用いて暗号化された前記コンテンツデータを前記データ提供装置から前記データ配給装置に提供し、前記データ配給装置は、前記提供されたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置は、前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

【００６７】また、本発明の第１２の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記管理装置から前記データ提供装置に配給し、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納した第１のモジュールを、前記データ提供装置から前記データ配給装置に提供し、前記提供を受けたコンテンツファイルおよび前記キーファイルを格納した第２のモジュールを前記データ配給装置から前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記第２のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第２のモジュールに格納された前記コンテンツデータの取り扱いを決定する。

【００６８】また、本発明の第１３の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと前記管理装置から受けたキーファイルとを含むコンテンツファイルを格納した第１のモジュールを前記データ配給装置に提供し、前記データ配給装置において、前記提供を受けたコンテンツファイルを格納した第２のモジュールを前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記第２のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復

号した権利書データに基づいて、前記配給を受けた前記第２のモジュールに格納された前記コンテンツデータの取り扱いを決定する。

【００６９】また、本発明の第１４の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記作成したキーファイルを前記管理装置から前記データ提供装置に配給し、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを個別に前記データ提供装置から前記データ配給装置に配給し、前記配給を受けた前記コンテンツファイルと前記キーファイルとを個別に前記データ配給装置から前記データ配給装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【００７０】また、本発明の第１５の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記管理装置から前記データ処理装置に配給し、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルを前記データ提供装置から前記データ配給装置に提供し、前記提供を受けたコンテンツファイルを前記データ配給装置から前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【００７１】また、本発明の第１６の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを格納した第１のモジュールを前記データ配給装置に提供し、前記データ配給装置において、前記提供を受けたコンテンツデータおよび前記キーファイルを格納した第２のモジュールを前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記第２のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記第２のモジュールに格納された前記コンテンツデータの取り扱いを決定する。

【００７２】また、本発明の第１７の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記キーファイルとを個別に前記データ配給装置に配給し、前記データ配給装置において、配給を受けた前記コンテンツデータと前記キーファイルとを個別に前記データ配給装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

【００７３】また、本発明の第１８の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に配給し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、前記データ配給装置において、前記提供を受けたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記

コンテンツデータの取り扱いを決定する。

【００７４】また、本発明の第１９の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ提供装置に提供し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータと、前記管理装置から受けた前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ配給装置に配給し、前記データ配給装置において、配給を受けた前記コンテンツデータと前記暗号化されたコンテンツ鍵データおよび前記暗号化された権利書データとを個別に前記データ配給装置に配給し、前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツデータの取り扱いを決定する。

【００７５】また、本発明の第２０の観点のデータ提供方法は、データ提供装置からデータ配給装置にコンテンツデータを提供し、前記データ配給装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置、前記データ配給装置および前記データ処理装置を管理するデータ提供方法であって、前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを前記データ処理装置に配給し、前記データ提供装置において、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けたコンテンツデータを前記データ処理装置に配給し、前記データ処理装置において、前記配給を受けた前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けた前記コンテンツデータの取り扱いを決定する。

【００７６】また、本発明の第２１の観点のデータ提供方法は、データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツのマスタソースデータを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスタソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルおよび前記キーファイルを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【００７７】また、本発明の第２２の観点のデータ提供方法は、データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツのマスタソースデータを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、前記提供されたマスタソースデータをコンテンツ鍵データを用いて暗号化してコンテンツデータを作成し、当該コンテンツデータを格納したコンテンツファイルを作成し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記コンテンツファイルを前記データ配給装置に提供し、前記キーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【００７８】また、本発明の第２３の観点のデータ提供方法は、データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルと、前記作成したキーファイルとを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルおよび前記キーファイルを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り

59

扱いを決定する。

【００７９】また、本発明の第２４の観点のデータ提供方法は、データ提供装置、データ配給装置、管理装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いた暗号化したコンテンツデータを格納したコンテンツファイルを前記管理装置に提供し、前記管理装置は、前記データ提供装置、前記データ配給装置および前記データ処理装置を管理し、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記データ提供装置から提供を受けた前記コンテンツファイルを前記データ配給装置に提供し、前記作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記提供を受けた前記コンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【００８０】また、本発明の第２５の観点のデータ提供方法は、データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ提供装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【００８１】また、本発明の第２６の観点のデータ提供方法は、データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの

60

取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記データ配給装置から提供を受けたキーファイルとを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【００８２】また、本発明の第２７の観点のデータ提供方法は、データ提供装置、データ配給装置、管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【００８３】また、本発明の第２８の観点のデータ提供方法は、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルおよび対応する前記管理装置から提供を受けたキーファイルを前記データベース装置に格納し、前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを対応する前記データ提供装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給

を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【００８４】また、本発明の第２９の観点のデータ提供方法は、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ配給装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【００８５】また、本発明の第３０の観点のデータ提供方法は、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツ鍵データを用いてコンテンツデータを暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データベース装置に格納し、前記管理装置は、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【００８６】また、本発明の第３１の観点のデータ提供方法は、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツデータのマスタソースを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルおよびキーファイルを前記データベースに格納し、前記管理装置は、対応する前記データ提供装置から受けた前記マスタソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、前記作成したコンテンツファイルおよび前記作成したキーファイルを対応する前記データ提供装置に送り、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルおよびキーファイルを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【００８７】また、本発明の第３２の観点のデータ提供方法は、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツデータのマスタソースを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記データベースに格納し、前記管理装置は、対応する前記データ提供装置から受けた前記マスタソースをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを対応する前記データ配給装置に送り、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルと、前記管理装置から提供を受けたキーファイルとを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【００８８】また、本発明の第３３の観点のデータ提供方法は、複数のデータ提供装置、データ配給装置、複数の管理装置、データベース装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置は、コンテンツデータのマスタソースを対応する前記管理装置に提供し、当該管理装置から受けたコンテンツファイルを前記データベースに格納し、前記管理装置は、対応する前記データ提供装置から受けた前記マスタソー

63

スをコンテンツ鍵データを用いて暗号化し、当該暗号化したコンテンツデータを格納したコンテンツファイルを作成し、当該作成したコンテンツファイルを前記データ提供装置に送り、対応する前記データ提供装置が提供するコンテンツデータについて、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、当該作成したキーファイルを前記データ処理装置に提供し、前記データ配給装置は、前記データベース装置から得た前記コンテンツファイルを前記データ処理装置に配給し、前記データ処理装置は、前記提供を受けた前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記配給を受けたコンテンツファイルに格納されたコンテンツデータの取り扱いを決定する。

【００８９】

【発明の実施の形態】以下、本発明の実施形態に係わるＥＭＤ（Ｅｌｅｃｔｒｏｎｉｃ　ＭｕｓｉｃＤｉｓｔｒｉｂｕｔｉｏｎ：電子音楽配信）システムについて説明する。

第１実施形態

図１は、本実施形態のＥＭＤシステム１００の構成図である。本実施形態において、ユーザに配信されるコンテンツ（Ｃｏｎｔｅｎｔ）データとは、情報そのものが価値を有するデジタルデータをいい、以下、音楽データを例に説明する。図１に示すように、ＥＭＤシステム１００は、コンテンツプロバイダ１０１、ＥＭＤサービスセンタ（クリアリング・ハウス、以下、ＥＳＣとも記す）１０２およびユーザホームネットワーク１０３を有する。ここで、コンテンツプロバイダ１０１、ＥＭＤサービスセンタ１０２およびＳＡＭ１０５$_1$～１０５$_4$が、それぞれ請求項１および請求項６などに係わるデータ提供装置、管理装置およびデータ処理装置に対応している。先ず、ＥＭＤシステム１００の概要について説明する。ＥＭＤシステム１００では、コンテンツプロバイダ１０１は、自らが提供しようとするコンテンツのコンテンツデータＣを暗号化する際に用いたコンテンツ鍵データＫｃ、コンテンツデータＣの使用許諾条件などの権利内容を示す権利書（ＵＣＰ：Ｕｓａｇｅ　Ｃｏｎｔｒｏｌ　Ｐｏｌｉｃｙ）データ１０６、並びに電子透かし情報の内容および埋め込み位置を示す電子透かし情報管理データを、高い信頼性のある権威機関であるＥＭＤサービスセンタ１０２に送る。

【００９０】ＥＭＤサービスセンタ１０２は、コンテンツプロバイダ１０１から受けたコンテンツ鍵データＫｃ、権利書データ１０６並びに電子透かし情報鍵データを登録（認証および権威化）する。また、ＥＭＤサービスセンタ１０２は、対応する期間の配信用鍵データＫＤ$_1$～ＫＤ５$_6$で暗号化したコンテンツ鍵データＫｃ、権

64

利書データ１０６および自らの署名データなどを格納したキーファイルＫＦを作成し、これをコンテンツプロバイダ１０１に送る。ここで、当該署名データは、キーファイルＫＦの改竄の有無、キーファイルＫＦの作成者の正当性およびキーファイルＫＦがＥＭＤサービスセンタ１０２において正規に登録されたことを検証するために用いられる。

【００９１】また、コンテンツプロバイダ１０１は、コンテンツ鍵データＫｃでコンテンツデータＣを暗号化してコンテンツファイルＣＦを生成し、当該生成したコンテンツファイルＣＦと、ＥＭＤサービスセンタ１０２から受けたキーファイルＫＦと、自らの署名データなどを格納したセキュアコンテナ（本発明のモジュール）１０４を、インターネットなどのネットワーク、デジタル放送あるいは記録媒体などのパッケージメディアを用いて、ユーザホームネットワーク１０３に配給する。ここで、セキュアコンテナ１０４内に格納された署名データは、対応するデータの改竄の有無、当該データの作成者および送信者の正当性を検証するために用いられる。

【００９２】ユーザホームネットワーク１０３は、例えば、ネットワーク機器１６０$_1$およびＡＶ機器１６０$_2$～１６０$_4$を有する。ネットワーク機器１６０$_1$は、ＳＡＭ（Ｓｅｃｕｒｅ　Ａｐｐｌｉｃａｔｉｏｎ　Ｍｏｄｕｌｅ）１０５$_1$を内蔵している。ＡＶ機器１６０$_2$～１６０$_4$は、それぞれＳＡＭ１０５$_2$～１０５$_4$を内蔵している。ＳＡＭ１０５$_1$～１０５$_4$相互間は、例えば、ＩＥＥＥ（Ｉｎｓｔｉｔｕｔｅ　ｏｆ　Ｅｌｅｃｔｒｉｃａｌ　ａｎｄ　Ｅｌｅｃｔｒｏｎｉｃｓ　Ｅｎｇｉｎｅｅｒｓ）１３９４シリアルインタフェースバスなどのバス１９１を介して接続されている。

【００９３】ＳＡＭ１０５$_1$～１０５$_4$は、ネットワーク機器１６０$_1$がコンテンツプロバイダ１０１からネットワークなどを介してオンラインで受信したセキュアコンテナ１０４、および／または、コンテンツプロバイダ１０１からＡＶ機器１６０$_2$～１６０$_4$に記録媒体を介してオフラインで供給されたセキュアコンテナ１０４を対応する期間の配信用鍵データＫＤ$_1$～ＫＤ$_3$を用いて復号した後に、署名データの検証を行う。ＳＡＭ１０５$_1$～１０５$_4$に供給されたセキュアコンテナ１０４は、ネットワーク機器１６０$_1$およびＡＶ機器１６０$_2$～１６０$_4$において、ユーザの操作に応じて購入・利用形態が決定された後に、再生や記録媒体への記録などの対象となる。ＳＡＭ１０５$_1$～１０５$_4$は、上述したセキュアコンテナ１０４の購入・利用の履歴を利用履歴（Ｕｓａｇｅ　Ｌｏｇ）データ１０８として記録すると共に、購入形態を示す利用制御状態データ１６６を作成する。利用履歴データ１０８は、例えば、ＥＭＤサービスセンタ１０２からの要求に応じて、ユーザホームネットワーク１０３からＥＭＤサービスセンタ１０２に送信される。利用制御状態データ１６６は、例えば、購入形態が

65

決定される度に、ユーザホームネットワーク１０３からＥＭＤサービスセンタ１０２に送信される。

【００９４】ＥＭＤサービスセンタ１０２は、利用履歴データ１０８に基づいて、課金内容を決定（計算）し、その結果に基づいて、ペイメントゲートウェイ９０を介して銀行などの決済機関９１に決済を行なう。これにより、ユーザホームネットワーク１０３のユーザが決済機関９１に支払った金銭が、ＥＭＤサービスセンタ１０２による決済処理によって、コンテンツプロバイダ１０１に支払われる。また、ＥＭＤサービスセンタ１０２は、一定期間毎に、決済レポートデータ１０７をコンテンツプロバイダ１０１に送信する。

【００９５】本実施形態では、ＥＭＤサービスセンタ１０２は、認証機能、鍵データ管理機能および権利処理（利益分配）機能を有している。すなわち、ＥＭＤサービスセンタ１０２は、中立の立場にある最高の権威機関であるルート認証局９２に対しての（ルート認証局９２の下層に位置する）セカンド認証局（Ｓｅｃｏｎｄ　Ｃｅｒｔｉｆｉｃａｔｅ　Ａｕｔｈｏｒｉｔｙ）としての役割を果たし、コンテンツプロバイダ１０１およびＳＡＭ１０５$_1$～１０５$_4$において署名データの検証処理に用いられる公開鍵データの公開鍵証明書データに、ＥＭＤサービスセンタ１０２の秘密鍵データによる署名を付けることで、当該公開鍵データの正当性を認証する。また、前述したように、ＥＭＤサービスセンタ１０２は、コンテンツプロバイダ１０１の権利書データ１０６を登録して権威化することも、ＥＭＤサービスセンタ１０２の認証機能の一つである。また、ＥＭＤサービスセンタ１０２は、例えば、配信用鍵データＫＤ$_1$～ＫＤ$_6$などの鍵データの管理を行なう鍵データ管理機能を有する。また、ＥＭＤサービスセンタ１０２は、権威化した権利書データ１０６に記述された標準小売価格ＳＲＰ（Ｓｕｇｇｅｓｔｅｄ　Ｒｅｔａｉｌｅｒ’　Ｐｒｉｃｅ）とＳＡＭ１０５$_1$～ＳＡＭ１０５$_4$から入力した利用履歴データ１０８とに基づいて、ユーザによるコンテンツの購入・利用に対して決済を行い、ユーザが支払った金銭をコンテンツプロバイダ１０１に分配する権利処理（利益分配）機能を有する。

【００９６】図２は、セキュアコンテナ１０４の概念をまとめた図である。図２に示すように、セキュアコンテナ１０４には、コンテンツプロバイダ１０１が作成したコンテンツファイルＣＦと、ＥＭＤサービスセンタ１０２が作成したキーファイルＫＦとが格納されている。コンテンツファイルＣＦには、ヘッダ部およびコンテンツＩＤを含むヘッダデータと、コンテンツ鍵データＫｃを用いた暗号化されたコンテンツデータＣと、これらについてのコンテンツプロバイダ１０１の秘密鍵データＫ$_{CP,S}$を用いた署名データとが格納されている。キーファイルＫＦには、ヘッダ部およびコンテンツＩＤを含むヘッダデータと、配信用鍵データＫＤ$_1$～ＫＤ$_6$によって暗号化されたコンテンツ鍵データＫｃおよび権利書データ１０６と、これらについてのＥＭＤサービスセンタ１０２の秘密鍵データＫ$_{ESC.S}$による署名データとが格納されている。

66

【００９７】以下、コンテンツプロバイダ１０１の各構成要素について詳細に説明する。

〔コンテンツプロバイダ１０１〕図３は、コンテンツプロバイダ１０１の機能ブロック図であり、ユーザホームネットワーク１０３のＳＡＭ１０５$_1$～１０５$_4$との間で送受信されるデータに関連するデータの流れが示されている。また、図４には、コンテンツプロバイダ１０１とＥＭＤサービスセンタ１０２との間で送受信されるデータに関連するデータの流れが示されている。なお、図４以降の図面では、署名データ処理部、および、セッション鍵データＫ$_{SES}$を用いた暗号化・復号部に入出力するデータの流れは省略している。

【００９８】図３および図４に示すように、コンテンツプロバイダ１０１は、コンテンツマスタソースデータベース１１１、電子透かし情報付加部１１２、圧縮部１１３、暗号化部１１４、乱数発生部１１５、伸長部１１６、署名処理部１１７、セキュアコンテナ作成部１１８、セキュアコンテナデータベース１１８ａ、キーファイルデータベース１１８ｂ、記憶部（データベース）１１９、相互認証部１２０、暗号化・復号部１２１、権利書データ作成部１２２、聴感検査部１２３、ＳＡＭ管理部１２４、ＥＭＤサービスセンタ管理部１２５およびコンテンツＩＤ生成部８５０を有する。コンテンツプロバイダ１０１は、ＥＭＤサービスセンタ１０２との間で通信を行う前に、例えば、自らが生成した公開鍵データ、自らの身分証明書および銀行口座番号（決済を行う口座番号）をオフラインでＥＭＤサービスセンタ１０２に登録し、自らの識別子（識別番号）ＣＰ＿ＩＤを得る。また、コンテンツプロバイダ１０１は、ＥＭＤサービスセンタ１０２から、ＥＭＤサービスセンタ１０２の公開鍵データと、ルート認証局９２の公開鍵データとを受ける。以下、図３および図４に示すコンテンツプロバイダ１０１の各機能ブロックについて説明する。

【００９９】コンテンツマスタソースデータベース１１１は、ユーザホームネットワーク１０３に提供するコンテンツのマスタソースであるコンテンツデータを記憶し、提供しようとするコンテンツデータＳ１１１を電子透かし情報付加部１１２に出力する。

【０１００】電子透かし情報付加部１１２は、コンテンツデータＳ１１１に対して、ソース電子透かし情報（Ｓｏｕｒｃｅ　Ｗａｔｅｒｍａｒｋ）Ｗｓ、コピー管理用電子透かし情報（Ｃｏｐｙ　Ｃｏｎｔｒｏｌ　Ｗａｔｅｒｍａｒｋ）Ｗｃ、ユーザ電子透かし情報（Ｕｓｅｒ　Ｗａｔｅｒｍａｒｋ）Ｗｕおよびリンク用電子透かし情報（Ｌｉｎｋ　Ｗａｔｅｒｍａｒｋ）ＷＬなどを埋め込んでコンテンツデータＳ１１２を生成し、コンテンツデ

ータＳ１１２を圧縮部１１３に出力する。

【０１０１】ソース電子透かし情報Ｗｓは、コンテンツデータの著作権者名、ＩＳＲＣコード、オーサリング日付、オーサリング機器ＩＤ（ＩｄｅｎｔｉｆｉｃａｔｉｏｎＤａｔａ）、コンテンツの配給先などの著作権に関する情報である。コピー管理用電子透かし情報Ｗｃは、アナログインタフェース経由でのコピー防止用のためのコピー禁止ビットを含む情報である。ユーザ電子透かし情報Ｗｕには、例えば、セキュアコンテナ１０４の配給元および配給先を特定するためのコンテンツプロバイダ１０１の識別子ＣＰ＿ＩＤおよびユーザホームネットワーク１０３のＳＡＭ１０５$_1$～１０５$_4$の識別子ＳＡＭ＿ＩＤ$_1$～ＳＡＭ＿ＩＤ$_4$が含まれる。リンク用電子透かし情報（Ｌｉｎｋ　Ｗａｔｅｒｍａｒｋ）ＷＬは、例えば、コンテンツデータＣのコンテンツＩＤを含んでいる。リンク用電子透かし情報ＷＬをコンテンツデータＣに埋め込むことで、例えば、テレビジョンやＡＭ／ＦＭラジオなどのアナログ放送でコンテンツデータＣが配信された場合でも、ユーザからの要求に応じて、ＥＭＤサービスセンタ１０２は、当該コンテンツデータＣを扱っているコンテンツプロバイダ１０１をユーザに紹介できる。すなち、当該コンテンツデータＣの受信先において、電子透かし情報デコーダを利用したコンテンツデータＣに埋め込まれたリンク用電子透かし情報ＷＬを検出し、当該検出したリンク用電子透かし情報ＷＬに含まれるコンテンツＩＤをＥＭＤサービスセンタ１０２に送信することで、ＥＭＤサービスセンタ１０２は当該ユーザに対して、当該コンテンツデータＣを扱っているコンテンツプロバイダ１０１などを紹介できる。

【０１０２】具体的には、例えば、車の中でユーザがラジオを聞きながら、放送中の曲が良いとユーザが思った時点で、所定のボタンを押せば、当該ラジオに内蔵されている電子透かし情報デコーダが、当該コンテンツデータＣに埋め込まれているリンク用電子透かし情報ＷＬに含まれるコンテンツＩＤや当該コンテンツデータＣを登録しているＥＭＤサービスセンタ１０２の通信アドレスなどを検出し、当該検出したデータをメモリスティックなどの半導体メモリやＭＤ（Ｍｉｎｉ　Ｄｉｓｋ）などの光ディスクなどの可搬メディアに搭載されているメディアＳＡＭに記録する。そして、当該可搬メディアをネットワークに接続されているＳＡＭを搭載したネットワーク機器をセットする。そして、当該ＳＡＭとＥＭＤサービスセンタ１０２とが相互認証を行った後に、メディアＳＡＭに搭載されている個人情報と、上記記録したコンテンツＩＤなどとをネットワーク機器からＥＭＤサービスセンタ１０２に送信する。その後、ネットワーク機器に、当該コンテンツデータＣを扱っているコンテンツプロバイダ１０１などの紹介リストなどを、ＥＭＤサービスセンタ１０２から受信する。また、その他に、例えば、ＥＭＤサービスセンタ１０２が、ユーザからコンテンツＩＤなどを受信したときに、当該コンテンツＩＤに対応したコンテンツデータＣを提供しているコンテンツプロバイダ１０１に当該ユーザを特定した情報を通知してもよい。この場合に、当該通信を受けたコンテンツプロバイダ１０１は、当該ユーザが契約者であれば、当該コンテンツデータＣをユーザのネットワーク機器に送信し、当該ユーザが契約者でなければ、自らに関するプロモーション情報をユーザのネットワーク機器に送信してもよい。

【０１０３】なお、後述する第２実施形態では、リンク用電子透かし情報ＷＬに基づいて、ＥＭＤサービスセンタ３０２は、ユーザに、当該コンテンツデータＣを扱っているサービスプロバイダ３１０を紹介できる。

【０１０４】また、本実施形態では、好ましくは、各々の電子透かし情報の内容と埋め込み位置とを、電子透かし情報モジュールＷＭとして定義し、ＥＭＤサービスセンタ１０２において電子透かし情報モジュールＷＭを登録して管理する。電子透かし情報モジュールＷＭは、例えば、ユーザホームネットワーク１０３内のネットワーク機器１６０$_1$およびＡＶ機器１６０$_2$～１６０$_4$が、電子透かし情報の正当性を検証する際に用いられる。例えば、ユーザホームネットワーク１０３では、ＥＭＤサービスセンタ１０２が管理するユーザ電子透かし情報モジュールに基づいて、電子透かし情報の埋め込み位置および埋め込まれた電子透かし情報の内容の双方が一致した場合に電子透かし情報が正当であると判断することで、偽りの電子透かし情報の埋め込みを高い確率で検出できる。

【０１０５】圧縮部１１３は、コンテンツデータＳ１１２を、例えば、ＡＴＲＡＣ３（Ａｄａｐｔｉｖｅ　Ｔｒａｎｓｆｏｒｍ　Ａｃｏｕｓｔｉｃ　Ｃｏｄｉｎｇ　３）（商標）などの音声圧縮方式で圧縮し、圧縮したコンテンツデータＳ１１３を暗号化部１１４に出力する。この場合に、圧縮部１１３による圧縮時に、コンテンツデータに対しての電子透かし情報の埋め込みを再び行ってもよい。具体的には、図３に示すように、伸長部１１６においてコンテンツデータ１１３を伸長してコンテンツデータＳ１１６を生成し、聴感検査部１２３においてコンテンツデータＳ１１６を再生したときに、電子透かし情報の埋め込みが音質に与える影響を、例えば実際に人間が聴いて判断し、所定の基準を満たさない場合には、電子透かし情報付加部１１２に電子透かし情報の埋め込み処理を再び行うように指示する。これにより、例えば、データの損失を伴う音声圧縮方式を採用したときに、当該圧縮によって、埋め込んだ電子透かし情報が落ちてしまった場合に適切に対処できる。また、圧縮したコンテンツデータを再度伸長して、埋め込みを行った電子透かし情報を正確に検出できるか否かの確認を行ってもよい。この場合に、音質聴感の検証も行い、聴感上問題がある場合には、電子透かし情報の埋め込みの調整を

69

行う。例えば、マスキング効果を利用して電子透かし情報を埋め込む場合には、電子透かし情報の埋め込みを行うレベルを調整する。

【０１０６】暗号化部１１４は、コンテンツ鍵データＫｃを共通鍵として用い、ＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）やＴｒｉｐｌｅ　ＤＥＳなどの共通鍵暗号化方式で、コンテンツデータＳ１１３を暗号化してコンテンツデータＣを生成し、これをセキュアコンテナ作成部１１８に出力する。また、暗号化部１１４は、コンテンツ鍵データＫｃを共通鍵として用い、Ａ／Ｖ伸長用ソフトウェアＳｏｆｔ、メタデータＭｅｔａおよび電子透かし情報管理データWMを暗号化した後に、セキュアコンテナ作成部１１７に出力する。

【０１０７】ＤＥＳは、５６ビットの共通鍵を用い、平文の６４ビットを１ブロックとして処理する暗号化方式である。ＤＥＳの処理は、平文を撹拌し、暗号文に変換する部分（データ撹拌部）と、データ撹拌部で使用する鍵（拡大鍵）データを共通鍵データから生成する部分（鍵処理部）とからなる。ＤＥＳの全てのアルゴリズムは公開されているので、ここでは、データ撹拌部の基本的な処理を簡単に説明する。

【０１０８】先ず、平文の６４ビットは、上位３２ビットのＨ$_0$と下位３２ビットのＬ$_0$とに分割される。鍵処理部から供給された４８ビットの拡大鍵データＫ$_1$および下位３２ビットのＬ$_0$を入力とし、下位３２ビットのＬ$_0$を撹拌したＦ関数の出力が算出される。Ｆ関数は、数値を所定の規則で置き換える「換字」およびビット位置を所定の規則で入れ替える「転置」の２種類の基本変換から構成されている。次に、上位３２ビットのＨ$_0$と、Ｆ関数の出力との排他的論理和が算出され、その結果はＬ$_1$とされる。また、Ｌ$_0$は、Ｈ$_1$とされる。そして、上位３２ビットのＨ$_0$および下位３２ビットのＬ$_0$を基に、以上の処理を１６回繰り返し、得られた上位３２ビットのＨ$_{16}$および下位３２ビットのＬ$_{16}$が暗号文として出力される。復号は、暗号化に使用した共通鍵データを用いて、上記の手順を逆さにたどることで実現される。

【０１０９】乱数発生部１１５は、所定ビット数の乱数を発生し、当該乱数をコンテンツ鍵データＫｃとして記憶部１１９に記憶する。なお、コンテンツ鍵データＫｃは、コンテンツデータが提供する楽曲に関する情報から生成してもよい。コンテンツ鍵データＫｃは、例えば、所定時間毎に更新される。また、複数のコンテンツプロバイダ１０１が存在する場合に、個々のコンテンツプロバイダ１０１によって固有のコンテンツ鍵データＫｃを用いてもよいし、全てのコンテンツプロバイダ１０１に共通のコンテンツ鍵データＫｃを用いてもよい。

【０１１０】キーファイルデータベース１１８ｂには、図４に示すように、ＥＭＤサービスセンタ管理部１２５を介してＥＭＤサービスセンタ１０２から受信した図５

70

（Ｂ）に示すキーファイルＫＦが記憶される。キーファイルＫＦは、コンテンツデータＣ毎に存在し、後述するように、コンテンツファイルＣＦのヘッダ内のディレクトリ構造データＤＳＤによって、対応するコンテンツファイルＣＦとの間でリンク関係が指定されている。キーファイルＫＦには、図５（Ｂ）および図７に示すように、ヘッダ、コンテンツ鍵データＫｃ、権利書データ（使用許諾条件）１０６、ＳＡＭプログラム・ダウンロード・コンテナＳＤＣ$_1$～ＳＤＣ$_3$および署名データＳＩＧ$_{K1,ESC}$が格納されている。ここで、コンテンツプロバイダ１０１の秘密鍵データＫ$_{ESC,S}$を用いた署名データは、図５（Ｂ）に示すようにキーファイルＫＦに格納される全てのデータに対しての署名データＫ$_{1,ESC}$にしてもよいし、図７に示すようにヘッダから鍵ファイルに関する情報までのデータに対しての署名データと、コンテンツ鍵データＫｃおよび権利書データ１０６に対しての署名データと、ＳＡＭプログラム・ダウンロード・コンテナＳＤＣに対しての署名データとを別々に設けてもよい。コンテンツ鍵データＫｃおよび権利書データ１０６と、ＳＡＭプログラム・ダウンロード・コンテナＳＤＣ$_1$～ＳＤＣ$_3$とは、それぞれ対応する期間の配信用鍵データＫＤ$_1$～ＫＤ$_6$を用いて暗号化されている。

【０１１１】ヘッダデータには、図７に示すように、同期信号、コンテンツＩＤ、コンテンツＩＤに対してのコンテンツプロバイダ１０１の秘密鍵データＫ$_{ESC,S}$による署名データ、ディレクトリ構造データ、ハイパーリンクデータ、キーファイルＫＦに関する情報、およびディレクトリ構造データ等に対してのコンテンツプロバイダ１０１の秘密鍵データＫ$_{ESC,S}$による署名データが含まれる。なお、ヘッダデータに含める情報としては種々の情報が考えられ、状況に応じて任意に変更可能である。例えば、ヘッダデータに、図８に示すような情報を含めてもよい。また、コンテンツＩＤには、例えば、図９に示す情報が含まれている。コンテンツＩＤは、ＥＭＤサービスセンタ１０２あるいはコンテンツプロバイダ１０１において作成され、ＥＭＤサービスセンタ１０２において作成された場合には図９に示すようにＥＭＤサービスセンタ１０２の秘密鍵データＫ$_{ESC,S}$による署名データが添付され、コンテンツプロバイダ１０１において作成された場合にはコンテンツプロバイダ１０１の秘密鍵データＫ$_{CP,S}$が添付される。コンテンツＩＤは、例えば、図４に示すように、コンテンツＩＤ生成部８５０が作成し、記憶部１１９に格納される。なお、コンテンツＩＤは、ＥＭＤサービスセンタ１０２が作成してもよい。

【０１１２】ディレクトリ構造データは、セキュアコンテナ１０４内におけるコンテンツファイルＣＦ相互間の対応関係と、コンテンツファイルＣＦとキーファイルＫＦとの対応関係を示している。例えば、セキュアコンテ

71

ナ１０４内にコンテンツファイルＣＦ$_1$～ＣＦ$_3$と、それらに対応するキーファイルＫＦ$_1$～ＫＦ$_3$が格納されている場合には、図１０に示すように、コンテンツファイルＣＦ$_1$～ＣＦ$_3$相互間のリンクと、コンテンツファイルＣＦ$_1$～ＣＦ$_3$とキーファイルＫＦ$_1$～ＫＦ$_3$との間のリンク関係とがディレクトリ構造データによって確立される。ハイパーリンクデータは、セキュアコンテナ１０４の内外の全てのファイルを対象として、キーファイルＫＦ相互間での階層構造と、コンテンツファイルＣＦとキーファイルＫＦとの対応関係を示している。具体的には、図１１に示すように、セキュアコンテナ１０４内にコンテンツファイルＣＦおよびキーファイルＫＦ毎のリンク先のアドレス情報とその認証値（ハッシュ値）とを格納し、ハッシュ関数Ｈ（ｘ）を用いて得た自らのアドレス情報のハッシュ値と、相手方の認証値とを比較してリンク関係を検証する。

【０１１３】また、権利書データ１０６には、図７に示すように、コンテンツＩＤ、コンテンツプロバイダ１０１の識別子ＣＰ＿ＩＤ、権利書データ１０６の有効期限、ＥＭＤサービスセンタ１０２の通信アドレス、利用空間調査情報、卸売価格情報、取扱方針、取扱制御情報、商品デモ（試聴）の取扱制御情報およびそれらについての署名データなどが含まれる。なお、後述する第２実施形態のように、サービスプロバイダ３１０を介してユーザホームネットワーク３０３にセキュアコンテナ３０４を送信する場合には、権利書データ１０６には、コンテンツプロバイダ３０１がセキュアコンテナ１０４を提供するサービスプロバイダ３１０の識別子ＳＰ＿ＩＤが含まれる。

【０１１４】また、ＳＡＭプログラム・ダウンロード・コンテナＳＤＣ$_1$～ＳＤＣ$_3$には、図７に示すように、ＳＡＭ１０５$_1$～１０５$_4$内でプログラムのダウンロードを行なう際に用いられるダウンロードの手順を示すダウンロード・ドライバと、権利書データ（ＵＣＰ）Ｕ１０６のシンタックス（文法）を示すＵＣＰ－Ｌ（Ｌａｂｅｌ），Ｒ（Ｒｅａｄｅｒ）などのラベルリーダと、ＳＡＭ１０５$_1$～１０５$_4$に内蔵された記憶部（フラッシュＲＯＭ）の書き換えおよび消去をブロック単位でロック状態／非ロック状態にするためのロック鍵データと、それらについての署名データとが含まれる。

【０１１５】なお、記憶部１１９は、例えば、公開鍵証明書データを記憶するデータベースを含む種々のデータベースを備えている。

【０１１６】署名処理部１１７は、署名を行なう対象となるデータのハッシュ値をとり、コンテンツプロバイダ１０１の秘密鍵データＫｃｐ，ｓを用いて、その署名データＳＩＧを作成する。

【０１１７】なお、ハッシュ値は、ハッシュ関数を用いて生成される。ハッシュ関数は、対象となるデータを入力とし、当該入力したデータを所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの１ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難であるという特徴を有している。

72

【０１１８】セキュアコンテナ作成部１１８は、図５（Ａ）に示すように、ヘッダデータと、暗号化部１１４から入力したそれぞれコンテンツ鍵データＫｃで暗号化されたメタデータＭｅｔａ、コンテンツデータＣ、Ａ／Ｖ伸長用ソフトウェアＳｏｆｔおよび電子透かし情報モジュール（Ｗａｔｅｒｍａｒｋ　Ｍｏｄｕｌｅ）ＷＭとを格納したコンテンツファイルＣＦを生成する。

【０１１９】コンテンツファイルＣＦには、図６に示すように、ファイルリーダと、秘密鍵データＫｃｐ，ｓによるファイルリーダの署名データとを含むようにしてもよい。このようにすることで、ＳＡＭ１０５$_1$～１０５$_4$において、異系列の複数のセキュアコンテナ１０４から受信したそれぞれ異なるフォーマットのコンテンツファイルＣＦを格納した複数のセキュアコンテナ１０４を効率的に処理できる。

【０１２０】ここで、ファイルリーダは、コンテンツファイルＣＦおよびそれに対応するキーファイルＫＦを読む際に用いられ、これらのファイルの読み込み手順などを示している。但し、本実施形態では、ＥＭＤサービスセンタ１０２からＳＡＭ１０５$_1$～１０５$_4$に、当該ファイルリーダを予め送信している場合を例示する。すなわち、本実施形態では、セキュアコンテナ１０４のコンテンツファイルＣＦは、ファイルリーダを格納していない。

【０１２１】ヘッダデータには、図６に示すように、同期信号、コンテンツＩＤ、コンテンツＩＤに対してのコンテンツプロバイダ１０１の秘密鍵データＫｃｐ，ｓによる署名データ、ディレクトリ情報、ハイパーリンク情報、シリアルナンバー、コンテンツファイルＣＦの有効期限並びに作成者情報、ファイルサイズ、暗号の有無、暗号アルゴリズム、署名アルゴリズムに関しての情報、およびディレクトリ情報などに関してのコンテンツプロバイダ１０１の秘密鍵データＫｃｐ，ｓによる署名データが含まれる。

【０１２２】メタデータＭｅｔａには、図６に示すように、商品（コンテンツデータＣ）の説明文、商品デモ宣伝情報、商品関連情報およびこれらについてのコンテンツプロバイダ１０１による署名データが含まれる。本発明では、図５および図６に示すように、コンテンツファイルＣＦ内にメタデータＭｅｔａを格納して送信する場合を例示するが、メタデータＭｅｔａをコンテンツファイルＣＦ内に格納せずに、コンテンツファイルＣＦを送信する経路とは別の経路でコンテンツプロバイダ１０１からＳＡＭ１０５$_1$などに送信してもよい。

【０１２３】Ａ／Ｖ伸長用ソフトウェアＳｏｆｔは、ユーザホームネットワーク１０３のネットワーク機器１６０$_1$およびＡＶ機器１６０$_2$～１６０$_4$において、コンテンツファイルＣＦを伸長する際に用いられるソフトウェアであり、例えば、ＡＴＲＡＣ３方式の伸長用ソフトウェアである。このように、セキュアコンテナ１０４内にＡ／Ｖ伸長用ソフトウェアＳｏｆｔを格納することで、ＳＡＭ１０５$_1$～１０５$_4$においてセキュアコンテナ１０４内に格納されたＡ／Ｖ伸長用ソフトウェアＳｏｆｔを用いてコンテンツデータＣの伸長を行うことができ、コンテンツデータＣ毎あるいはコンテンツプロバイダ１０１毎にコンテンツデータＣの圧縮および伸長方式をコンテンツプロバイダ１０１が自由に設定しても、ユーザに多大な負担をかけることはない。

【０１２４】電子透かし情報モジュールWMは、前述したように、例えば、コンテンツデータＣに埋め込まれた電子透かし情報を検出するのに必要は情報およびソフトウェアを含んでいる。

【０１２５】また、セキュアコンテナ作成部１１８は、上述した図５（Ａ）に示すコンテンツファイルＣＦと、当該コンテンツファイルＣＦの署名データＳＩＧ$_{6,CP}$と、キーファイルデータベース１１８ｂから読み出した当該コンテンツファイルＣＦに対応する図５（Ｂ）に示すキーファイルＫＦと、当該キーファイルＫＦの署名データＳＩＧ$_{7,CP}$と、記憶部１１９から読み出したコンテンツプロバイダ１０１の公開鍵証明書データＣＥＲ$_{CP}$と、当該公開鍵証明書データＣＥＲ$_{CP}$の署名データＳＩＧ$_{1,ESC}$とを格納したセキュアコンテナ１０４を生成する。

【０１２６】ここで、署名データＳＩＧ$_{6,CP}$は、セキュアコンテナ１０４の受信先において、コンテンツファイルＣＦの作成者および送信者の正当性を検証するために用いられる。ここで、署名データＳＩＧ$_{7,CP}$は、セキュアコンテナ１０４の受信先において、キーファイルＫＦの送信者の正当性を検証するために用いられる。なお、セキュアコンテナ１０４の受信先において、キーファイルＫＦの作成者の正当性の検証は、キーファイルＫＦ内の署名データＳＩＧ$_{K1,ESC}$に基づいて行われる。また、署名データＳＩＧ$_{K1,ESC}$は、キーファイルＫＦが、ＥＭＤサービスセンタ１０２に登録されているか否かを検証するためにも用いられる。

【０１２７】本実施形態では、コンテンツデータＣの圧縮方式、圧縮の有無、暗号化方式（共通鍵暗号化方式および公開鍵暗号化方式の何れの場合も含む）、コンテンツデータＣを得た信号の諸元（サンプリング周波数など）および署名データの作成方式（アルゴリズム）に依存しない形式で、暗号化されたコンテンツデータＣがセキュアコンテナ１０４内に格納されている。すなわち、これらの事項をコンテンツプロバイダ１０１が自由に決定できる。

【０１２８】また、セキュアコンテナ作成部１１８は、セキュアコンテナデータバース１１８ａに格納したセキュアコンテナ１０４を、ユーザからの要求に応じてＳＡＭ管理部１２４に出力する。このように、本実施形態では、コンテンツプロバイダ１０１の公開鍵データＫ$_{CP,P}$の公開鍵証明書ＣＥＲ$_{CP}$をセキュアコンテナ１０４に格納してユーザホームネットワーク１０３に送信するイン・バンド（Ｉｎ－ｂａｎｄ）方式を採用している。従って、ユーザホームネットワーク１０３は、公開鍵証明書ＣＥＲ$_{CP}$得るための通信をＥＭＤサービスセンタ１０２との間で行う必要がない。なお、本発明では、公開鍵証明書ＣＥＲ$_{CP}$をセキュアコンテナ１０４に格納しないで、ユーザホームネットワーク１０３がＥＭＤサービスセンタ１０２から公開鍵証明書ＣＥＲ$_{CP}$を得るアウト・オブ・バンド（Ｏｕｔ－Ｏｆ－ｂａｎｄ）方式を採用してもよい。

【０１２９】相互認証部１２０は、コンテンツプロバイダ１０１がＥＭＤサービスセンタ１０２およびユーザホームネットワーク１０３との間でオンラインでデータを送受信する際に、それぞれＥＭＤサービスセンタ１０２およびユーザホームネットワーク１０３との間で相互認証を行ってセッション鍵データ（共有鍵）Ｋ$_{SES}$を生成する。セッション鍵データＫ$_{SES}$は、相互認証を行う度に新たに生成される。

【０１３０】暗号化・復号部１２１は、コンテンツプロバイダ１０１がＥＭＤサービスセンタ１０２およびユーザホームネットワーク１０３にオンラインで送信するデータを、セッション鍵データＫ$_{SES}$を用いて暗号化する。また、暗号化・復号部１２１は、コンテンツプロバイダ１０１がＥＭＤサービスセンタ１０２およびユーザホームネットワーク１０３からオンラインで受信したデータを、セッション鍵データＫ$_{SES}$を用いて復号する。

【０１３１】権利書データ作成部１２２は、権利書データ１０６を作成し、これをＥＭＤサービスセンタ管理部１２５に出力する。権利書データ１０６は、コンテンツデータＣの運用ルールを定義した記述子（ディスクリプター）であり、例えば、コンテンツプロバイダ１０１の運用者が希望する標準小売価格ＳＲＰ（Ｓｕｇｇｅｓｔｅｄ　Ｒｅｔａｉｌｅｒ’　Ｐｒｉｃｅ）やコンテンツデータＣの複製ルールなどが記述されている。

【０１３２】ＳＡＭ管理部１２４は、セキュアコンテナ１０４を、オフラインおよび／またはオンラインでユーザホームネットワーク１０３に供給する。また、ＳＡＭ管理部１２４は、セキュアコンテナ１０４をオンラインでＳＡＭ１０５$_1$～１０５$_4$に配給する場合には、セキュアコンテナ１０４を送信する通信プロコトルとして、デジタル放送であればＭＨＥＧ（Ｍｕｌｔｉｍｅｄｉａ　ａｎｄ　Ｈｙｐｅｒｍｅｄｉａ　ｉｎｆｏｒｍａｔｉｏ

ｎ ｃｏｄｉｎｇ Ｅｘｐｅｒｔｓ Ｇｒｏｕｐ）プロトコルを用い、インターネットであればＸＭＬ／ＳＭＩＬ／ＨＴＭＬ（Ｈｙｐｅｒ ＴｅｘｔＭａｒｋｕｐ Ｌａｎｇｕａｇｅ）を用い、これらの通信プロトコル内に、セキュアコンテナ１０４を、符号化方式に依存しない形式でトンネリングして埋め込む。従って、通信プロトルとセキュアコンテナ１０４との間でフォーマットの整合性をとる必要性はなく、セキュアコンテナ１０４のフォーマットを柔軟に設定できる。なお、コンテンツプロバイダ１０１からユーザホームネットワーク１０３にセキュアコンテナ１０４を送信する際に用いる通信プロトコルは、上述したものには限定されず任意である。

【０１３３】図１２は、本実施形態で用いられるＲＯＭ型の記録媒体１３０$_1$を説明するための図である。図１２に示すように、ＲＯＭ型の記録媒体１３０$_1$は、ＲＯＭ領域１３１、セキュアＲＡＭ領域１３２およびメディアＳＡＭ１３３を有する。ＲＯＭ領域１３１には、図５（Ａ）に示したコンテンツファイルＣＦが記憶されている。また、セキュアＲＡＭ領域１３２は、記憶データに対してのアクセスに所定の許可（認証）が必要な領域であり、図５（Ｂ）、（Ｃ）に示したキーファイルＫＦおよび公開鍵証明書データＣＥＲ$_{CP}$と機器の種類に応じて固有の値を持つ記録用鍵データＫ$_{STR}$とを引数としてＭＡＣ（Ｍｅｓｓａｇｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｏｄｅ）関数を用いて生成した署名データと、当該キーファイルＫＦおよび公開鍵証明書データＣＥＲ$_{CP}$とを記録媒体に固有の値を持つメディア鍵データＫ$_{MED}$を用いて暗号化したデータとが記憶される。また、セキュアＲＡＭ領域１３２には、例えば、不正行為などで無効となったコンテンツプロバイダ１０１およびＳＡＭ１０５$_1$～１０５$_5$を特定する公開鍵証明書破棄データ（リボケーションリスト）が記憶される。また、セキュアＲＡＭ領域１３２には、後述するようにユーザホームネットワーク１０３のＳＡＭ１０５$_1$～１０５$_4$においてコンテンツデータＣの購入・利用形態が決定されたときに生成される利用制御状態（ＵＣＳ）データ１６６などが記憶される。これにより、利用制御状態データ１６６がセキュアＲＡＭ領域１３２に記憶されることで、購入・利用形態が決定したＲＯＭ型の記録媒体１３０$_1$となる。メディアＳＡＭ１３３には、例えば、ＲＯＭ型の記録媒体１３０$_1$の識別子であるメディアＩＤと、メディア鍵データＫ$_{MED}$とが記憶されている。メディアＳＡＭ１３３は、例えば、相互認証機能を有している。

【０１３４】本実施形態で用いるＲＯＭ型の記録媒体としては、例えば、図１２に示すものの他に、図１３に示すＲＯＭ型の記録媒体１３０$_2$および図１４に示すＲＯＭ型の記録媒体１３０$_3$なども考えられる。図１３に示すＲＯＭ型の記録媒体１３０$_2$は、ＲＯＭ領域１３１と認証機能を有するメディアＳＡＭ１３３とを有し、図１２に示すＲＯＭ型の記録媒体１３０$_1$のようにセキュアＲＡＭ領域１３２を備えていない。ＲＯＭ型の記録媒体１３０$_2$を用いる場合には、ＲＯＭ領域１３１にコンテンツファイルＣＦを記録し、メディアＳＡＭ１３３にキーファイルＫＦを記憶する。また、図１４に示すＲＯＭ型の記録媒体１３０$_3$は、ＲＯＭ領域１３１およびセキュアＲＡＭ領域１３２を有し、図１２に示すＲＯＭ型の記録媒体１３０$_1$のようにメディアＳＡＭ１３３を有していない。ＲＯＭ型の記録媒体１３０$_3$を用いる場合には、ＲＯＭ領域１３１にコンテンツファイルＣＦを記録し、セキュアＲＡＭ領域１３２にキーファイルＫＦを記録する。また、ＲＯＭ型の記録媒体１３０$_3$を用いる場合には、ＳＡＭとの間で相互認証は行わない。また、本実施形態ではＲＯＭ型の記録媒体の他にＲＡＭ型の記録媒体も用いられる。

【０１３５】本実施形態で用いるＲＡＭ型の記録媒体としては、例えば図１５に示すように、メディアＳＡＭ１３３、セキュアＲＡＭ領域１３２およびセキュアでないＲＡＭ領域１３４を有するＲＡＭ型の記録媒体１３０$_4$がある。ＲＡＭ型の記録媒体１３０$_4$では、メディアＳＡＭ１３３は認証機能を持ち、キーファイルＫＦを記憶する。また、ＲＡＭ領域１３４には、コンテンツファイルＣＦが記録される。また、本実施形態で用いるＲＡＭ型の記録媒体としては、その他に、図１６に示すＲＡＭ型の記録媒体１３０$_5$および図１７に示すＲＡＭ型の記録媒体１３０$_6$なども考えられる。図１６に示すＲＡＭ型の記録媒体１３０$_5$は、セキュアでないＲＡＭ領域１３４と認証機能を有するメディアＳＡＭ１３３とを有し、図１５に示すＲＡＭ型の記録媒体１３０$_4$のようにセキュアＲＡＭ領域１３２を備えていない。ＲＡＭ型の記録媒体１３０$_5$を用いる場合には、ＲＡＭ領域１３４にコンテンツファイルＣＦを記録し、メディアＳＡＭ１３３にキーファイルＫＦを記憶する。また、図１７に示すＲＡＭ型の記録媒体１３０$_6$は、セキュアＲＡＭ領域１３２およびセキュアでないＲＡＭ領域１３４を有し、図１５に示すＲＡＭ型の記録媒体１３０$_4$のようにメディアＳＡＭ１３３を有していない。ＲＡＭ型の記録媒体１３０$_6$を用いる場合には、ＲＡＭ領域１３４にコンテンツファイルＣＦを記録し、セキュアＲＡＭ領域１３２にキーファイルＫＦを記録する。また、ＲＡＭ型の記録媒体１３０$_6$を用いる場合には、ＳＡＭとの間で相互認証は行わない。

【０１３６】また、ＳＡＭ管理部１２４は、セキュアコンテナ１０４を、ネットワークやデジタル放送などを用いてオンラインでユーザホームネットワーク１０３に配信する場合には、暗号化・復号部１２１においてセッション鍵データＫ$_{SES}$を用いてセキュアコンテナ１０４を暗号化した後に、ネットワークを介してユーザホームネットワーク１０３に配信する。本実施形態では、ＳＡＭ管理部、ＥＭＤサービスセンタ管理部、並びに後述す

るコンテンツプロバイダ管理部およびサービスプロバイダ管理部として、例えば、内部の処理内容の監視（モニタリング）および改竄ができないあるいは困難な耐タンパ性の構造を持つ通信ゲートウェイが用いられる。

【０１３７】ここで、コンテンツプロバイダ１０１からユーザホームネットワーク１０３へのコンテンツデータＣの配給は、上述したように記録媒体１３０$_1$を用いて行う場合とネットワークを使ってオンラインで行う場合との何れでも権利書データ１０６が格納された共通の形式のセキュアコンテナ１０４を用いる。従って、ユーザホームネットワーク１０３のＳＡＭ１０５$_1$～１０５$_4$では、オフラインおよびオンラインの何れの場合でも、共通の権利書データ１０６に基づいた権利処理を行なうことができる。

【０１３８】また、上述したように、本実施形態では、セキュアコンテナ１０４内に、コンテンツ鍵データＫｃで暗号化されたコンテンツデータＣと、当該暗号化を解くためのコンテンツ鍵データＫｃとを同封するイン・バンド（Ｉｎ－Ｂａｎｄ）方式を採用している。イン・バンド方式では、ユーザホームネットワーク１０３の機器で、コンテンツデータＣを再生しようとするときに、コンテンツ鍵データＫｃを別途配信する必要がなく、ネットワーク通信の負荷を軽減できるという利点がある。また、コンテンツ鍵データＫｃは配信用鍵データＫＤ$_1$～ＫＤ$_6$で暗号化されているが、配信用鍵データＫＤ$_1$～ＫＤ$_6$は、ＥＭＤサービスセンタ１０２で管理されており、ユーザホームネットワーク１０３のＳＡＭ１０５$_1$～１０５$_5$に事前に（ＳＡＭ１０５$_1$～１０５$_4$がＥＭＤサービスセンタ１０２に初回にアクセスする際に）配信されているので、ユーザホームネットワーク１０３では、ＥＭＤサービスセンタ１０２との間をオンラインで接続することなく、オフラインで、コンテンツデータＣの利用が可能になる。なお、本発明は、後述するようにコンテンツデータＣとコンテンツ鍵データＫｃとを別々に、ユーザホームネットワーク１０３に供給するアウト・オブ・バンド（Ｏｕｔ－Ｏｆ－Ｂａｎｄ）方式を採用できる柔軟性を有している。

【０１３９】ＥＭＤサービスセンタ管理部１２５は、ＥＭＤサービスセンタ１０２から決済レポートデータ１０７を受信すると、これらを暗号化・復号部１２１においてセッション鍵データＫ$_{SES}$を用いて復号した後に、記憶部１１９に記憶する。決済レポートデータ１０７は、例えば、ＥＭＤサービスセンタ１０２が図１に示す決済機関９１に対して行なったコンテンツプロバイダ１０１に関する決済の内容が記述されている。

【０１４０】また、ＥＭＤサービスセンタ管理部１２５は、提供するコンテンツデータＣのグローバルユニーク（Ｇｌｏｂａｌ　Ｕｎｉｑｕｅ）な識別子であるコンテンツＩＤ、公開鍵データＫ$_{CP,P}$およびそれらの署名データＳＩＧ$_{S,CP}$を、ＥＭＤサービスセンタ１０２に送信し、ＥＭＤサービスセンタ１０２から、公開鍵データＫ$_{CP,P}$の公開鍵証明書データＣＥＲ$_{CP}$を入力する。また、ＥＭＤサービスセンタ管理部１２５は、コンテンツデータＣのそれぞれについて、コンテンツ鍵データＫｃ、権利書データ１０６および電子透かし情報管理データＷＭをＥＭＤサービスセンタ１０２に登録してキーファイルＫＦを受ける際に、図１８に示すように、提供するコンテンツデータＣのグローバルユニークな識別子であるコンテンツＩＤ、コンテンツ鍵データＫｃ、権利書データ１０６、電子透かし情報管理データＷＭ、コンテンツプロバイダ１０１のグローバルユニークな識別子であるＣＰ＿ＩＤと、それらについてのコンテンツプロバイダ１０１の秘密鍵データＫ$_{CP,S}$による署名データＳＩＧ$_{M1,CP}$とを格納した登録モジュールＭｏｄ$_2$を作成する。そして、ＥＭＤサービスセンタ管理部１２５は、登録モジュールＭｏｄ$_2$を暗号化・復号部１２１においてセッション鍵データＫ$_{SES}$を用いて暗号化した後に、ネットワークを介してＥＭＤサービスセンタ１０２に送信する。ＥＭＤサービスセンタ管理部１２５としては、前述したように、例えば、内部の処理内容の監視（モニタリング）および改竄ができないあるいは困難な耐タンパ性の構造を持つ通信ゲートウェイが用いられる。

【０１４１】以下、図３および図４を参照しながら、コンテンツプロバイダ１０１における処理の流れを説明する。なお、以下に示す処理を行う前提として、コンテンツプロバイダ１０１の関係者は、例えば、自らの身分証明書および決済処理を行う銀行口座などを用いて、オフラインで、ＥＭＤサービスセンタ１０２に登録処理を行い、グローバルユニークな識別子ＣＰ＿ＩＤを得ている。識別子ＣＰ＿ＩＤは、記憶部１１９に記憶されている。

【０１４２】先ず、コンテンツプロバイダ１０１が、ＥＭＤサービスセンタ１０２に、自らの秘密鍵データＫ$_{CP,S}$に対応する公開鍵データＫ$_{CP,S}$の正当性を証明する公開鍵証明書データＣＥＲ$_{CP}$を要求する場合の処理を図４を参照しながら説明する。コンテンツプロバイダ１０１は、真性乱数発生器を用いて乱数を発生して秘密鍵データＫ$_{CP,S}$を生成し、当該秘密鍵データＫ$_{CP,S}$に対応する公開鍵データＫ$_{CP,P}$を作成して記憶部１１９に記憶する。ＥＭＤサービスセンタ管理部１２５は、コンテンツプロバイダ１０１の識別子ＣＰ＿ＩＤおよび公開鍵データＫ$_{CP,P}$を記憶部１１９から読み出す。そして、ＥＭＤサービスセンタ管理部１２５は、識別子ＣＰ＿ＩＤおよび公開鍵データＫ$_{CP,P}$を、ＥＭＤサービスセンタ１０２に送信する。そして、ＥＭＤサービスセンタ管理部１２５は、当該登録に応じて、公開鍵証明書データＣＥＲ$_{CP}$およびその署名データＳＩＧ$_{1,ESC}$をＥＭＤサービスセンタ１０２から入力して記憶部１１９に書き込む。

79

【０１４３】次に、コンテンツプロバイダ１０１が、ＥＭＤサービスセンタ１０２にコンテンツ鍵データＫｃ、権利書データ１０６および電子透かし情報管理データＷＭを登録し、コンテンツデータＣに対応するキーファイルＫＦを受信する場合の処理を図４、図１８および図１９を参照して説明する。権利書データ１０６などの登録は、個々のコンテンツデータＣについてそれぞれ行われる。図１９は、コンテンツプロバイダ１０１からＥＭＤサービスセンタ１０２への登録処理を説明するためのフローチャートである。

【０１４４】ステップＡ１：図４に示すコンテンツプロバイダ１０１の相互認証部１２０とＥＭＤサービスセンタ１０２との間で相互認証を行う。

ステップＡ２：ステップＡ１で行った相互認証によって得られたセッション鍵データK_{SES}をコンテンツプロバイダ１０１およびＥＭＤサービスセンタ１０２で共有する。

【０１４５】ステップＡ３：コンテンツプロバイダ１０１は、記憶部１１９などのデータベースから、ＥＭＤサービスセンタ１０２に登録を行うコンテンツＩＤ、コンテンツ鍵データＫｃ、権利書データ１０６、電子透かし情報管理データＷＭおよびＣＰ＿ＩＤなどを読み出す。

ステップＡ４：署名処理部１１７において、コンテンツプロバイダ１０１の秘密鍵データ$K_{CP,S}$を用いて、ステップＡ３で読み出した権利書データ１０６などを含むモジュールに対して、送り主の正当性を示す署名データ$SIG_{M1,CP}$を作成する。そして、ＥＭＤサービスセンタ管理部１２５は、図１８に示すように、コンテンツＩＤ、コンテンツ鍵データＫｃ、権利書データ１０６、電子透かし情報管理データＷＭおよびＣＰ＿ＩＤと、これらについての署名データ$SIG_{M1,CP}$とを格納した登録用モジュールMod_2を作成する。

【０１４６】ステップＡ５：暗号化・復号部１２１は、ステップＡ４で作成した登録用モジュールMod_2を、ステップＡ２で共有したセッション鍵データK_{SES}を用いて暗号化する。

ステップＡ６：ＥＭＤサービスセンタ管理部１２５は、ステップＡ５で暗号化した登録用モジュールMod_2をＥＭＤサービスセンタ１０２に送信する。

【０１４７】ステップＡ７以降の処理は、ＥＭＤサービスセンタ１０２における処理である。

ステップＡ７：ＥＭＤサービスセンタ１０２は、受信した登録用モジュールMod_2を、ステップＡ２において共有したセッション鍵データK_{SES}を用いて復号する。

ステップＡ８：ＥＭＤサービスセンタ１０２は、復号した登録用モジュールMod_2に格納された署名データ$SIG_{M1,CP}$を公開鍵データ$K_{CP,P}$を用いて検証し、登録用モジュールMod_2の送り主の正当性を確認し、送り主の正当性が証明されたことを条件にステップＡ９の処理を行う。

80

ステップＡ９：ＥＭＤサービスセンタ１０２は、登録用モジュールMod_2に格納されているコンテンツＩＤ、コンテンツ鍵データＫｃ、権利書データ１０６、電子透かし情報管理データＷＭおよびＣＰ＿ＩＤを所定のデータベースに格納して登録する。

【０１４８】なお、ＥＭＤサービスセンタ管理部１２５は、図１８に示すように、登録用モジュールMod_2に応じた登録処理がＥＭＤサービスセンタ１０２に行われた後に、例えば６カ月分のキーファイルＫＦをＥＭＤサービスセンタ１０２から受信し、相互認証部１２０とＥＭＤサービスセンタ１０２との間の相互認証によって得たセッション鍵データK_{SES}を用いて、当該受信したキーファイルＫＦを復号した後にキーファイルデータベース１１８ｂに記憶する。

【０１４９】次に、コンテンツプロバイダ１０１がユーザホームネットワーク１０３のＳＡＭ105_1にセキュアコンテナ１０４を送信する場合の処理を図３および図４を参照しながら説明する。なお、以下の例では、コンテンツプロバイダ１０１から$SAM105_1$にセキュアコンテナ１０４を送信する場合を例示するが、セキュアコンテナ１０４を$SAM105_2$～105_4に送信する場合も、$SAM105_1$を介して$SAM105_2$～105_4に送信される点を除いて同じである。先ず、図３に示すように、コンテンツデータＳ１１１がコンテンツマスタソースデータベース１１１から読み出されて電子透かし情報付加部１１２に出力される。次に、電子透かし情報付加部１１２は、コンテンツデータＳ１１１に電子透かし情報を埋め込んでコンテンツデータＳ１１２を生成し、これを圧縮部１１３に出力する。次に、圧縮部１１３は、コンテンツデータＳ１１２を、例えばＡＴＲＡＣ３方式で圧縮してコンテンツデータＳ１１３を作成し、これを暗号化部１１４に出力する。また、図４に示すように、乱数発生部１１５において、乱数を発生してコンテンツ鍵データＫｃが生成され、当該生成されたコンテンツ鍵データＫｃが記憶部１１９に記憶される。

【０１５０】次に、暗号化部１１４は、圧縮部１１３から入力したコンテンツデータＳ１１３と、記憶部１１９から読み出したメタデータＭｅｔａ、Ａ／Ｖ伸長用ソフトウェアＳｏｆｔおよび電子透かし情報管理データＷＭとを、コンテンツ鍵データＫｃを用いて暗号化してセキュアコンテナ作成部１１８に出力する。この場合に、メタデータＭｅｔａおよび電子透かし情報管理データＷＭは暗号化しなくてもよい。そして、セキュアコンテナ作成部１１８は、図５（Ａ）に示すコンテンツファイルＣＦを作成する。また、署名処理部１１７において、コンテンツファイルＣＦのハッシュ値がとられ、秘密鍵データ$K_{CP,S}$を用いて署名データ$SIG_{6,CP}$が生成される。

【０１５１】また、セキュアコンテナ作成部１１８は、

81

キーファイルデータベース１１８ｂから、コンテンツデータＣに対応するキーファイルＫＦを読み出し、これを署名処理部１１７に出力する。そして、署名処理部１１７は、セキュアコンテナ作成部１１８から入力したキーファイルＫＦのハッシュ値をとり、秘密鍵データＫｃｐ，ｓを用いて署名データＳＩＧ７，ｃｐを生成し、これをセキュアコンテナ作成部１１８に出力する。次に、セキュアコンテナ作成部１１８は、図５（Ａ）に示すコンテンツファイルＣＦおよびその署名データＳＩＧ６，ｃｐと、図５（Ｂ）に示すキーファイルＫＦおよびその署名データＳＩＧ７，ｃｐと、記憶部１１９から読み出した図５（Ｃ）に示す公開鍵証明書データＣＥＲｃｐおよびその署名データＳＩＧ１，Ｅｓｃとを格納したセキュアコンテナ１０４を作成し、これを、セキュアコンテナデータベース１１８ａに記憶する。そして、セキュアコンテナ作成部１１８は、例えばユーザからの要求（リクエスト）に応じてユーザホームネットワーク１０３に提供しようとするセキュアコンテナ１０４をセキュアコンテナデータベース１１８ａから読み出して、相互認証部１２０とＳＡＭ１０５１との間の相互認証によって得られたセッション鍵データＫｓＥｓを用いて暗号化・復号部１２１において暗号化した後に、ＳＡＭ管理部１２４を介してユーザホームネットワーク１０３のＳＡＭ１０５１に送信する。

【０１５２】以下、コンテンツプロバイダ１０１の処理の全体の流れの概要を、セキュアコンテナ作成処理と関連付けて述べる。図２０，図２１，図２２は、当該処理の流れを説明するためのフローチャートである。

ステップＢ１：コンテンツプロバイダ１０１は、予め自らの公開鍵証明書データＣＥＲｃｐをＥＭＤサービスセンタ１０２から入力し、記憶部（データベース）１１９に格納しておく。

ステップＢ２：新しくオーサリングするコンテンツデータや、既に保管されているレガシーコンテンツデータなどのコンテンツマスタソースをデジタル化し、さらにコンテンツＩＤを割り振り、コンテンツマスタソースデータベース１１１に格納して一元的に管理する。

ステップＢ３：ステップＢ１において一元的に管理した各々のコンテンツマスタソースにメタデータＭｅｔａを作成し、これを記憶部１１９に格納する。

【０１５３】ステップＢ４：コンテンツマスタソースデータベース１１１からコンテンツマスタソースであるコンテンツデータＳ１１１を読み出して電子透かし情報付加部１１２に出力し、電子透かし情報を埋め込んでコンテンツデータＳ１１２を生成する。

ステップＢ５：電子透かし情報付加部１１２は、埋め込みを行った電子透かし情報の内容と埋め込み位置とを所定のデータベースに格納する。

ステップＢ６：圧縮部１１３において、電子透かし情報が埋め込まれたコンテンツデータＳ１１２を圧縮してコンテンツデータＳ１１３を生成する。

82

ステップＢ７：伸長部１１６において、圧縮されたコンテンツデータＳ１１３を伸長してコンテンツデータＳ１１６を生成する。

ステップＢ８：聴感検査部１２３において、伸長したコンテンツデータＳ１１６の聴覚検査を行う。

ステップＢ９：コンテンツプロバイダ１０１は、コンテンツデータＳ１１６に埋め込まれた電子透かし情報を、ステップＢ５でデータベースに格納した埋め込み内容および埋め込み位置に基づいて検出する。そして、コンテンツプロバイダ１０１は、聴覚検査および電子透かし情報の検出の双方が成功した場合には、ステップＢ１０の処理を行い、何れか一方が失敗した場合にはステップＢ４の処理を繰り返す。

【０１５４】ステップＢ１０：乱数発生部１１５において乱数してコンテンツ鍵データＫｃを生成し、これを記憶部１１９に格納する。

ステップＢ１１：暗号化部１１４において、圧縮したコンテンツデータＳ１１３を、コンテンツ鍵データＫｃを用いて暗号化してコンテンツデータＣを作成する。

【０１５５】ステップＢ１２：権利書データ作成部１２２において、コンテンツデータＣについての権利書データ１０６を作成する。

ステップＢ１３：コンテンツプロバイダ１０１は、ＳＲＰを決定し、これを記憶部１１９に格納する。

ステップＢ１４：コンテンツプロバイダ１０１は、コンテンツＩＤ、コンテンツ鍵データＫｃおよび権利書データ１０６をＥＭＤサービスセンタ１０２に出力する。

ステップＢ１５：コンテンツプロバイダ１０１は、配信用鍵データＫＤ１～ＫＤ３で暗号化されたキーファイルＫＦをＥＭＤサービスセンタ１０２から入力する。

ステップＢ１６：コンテンツプロバイダ１０１は、入力したキーファイルＫＦをキーファイルデータベース１１８ｂに格納する。

【０１５６】ステップＢ１７：コンテンツプロバイダ１０１は、コンテンツデータＣとキーファイルＫＦとのリンク関係をハイパーリンクで結ぶ。

ステップＢ１８：署名処理部１１７において、コンテンツデータＣおよびキーファイルＫＦの各々について、秘密鍵データＫｃｐ，ｓを用いて、作成者の正当性を署名データを作成する。

ステップＡ１９：セキュアコンテナ作成部１１８において、図５に示すセキュアコンテナ１０４を作成する。

【０１５７】ステップＢ２０：複数のセキュアコンテナを用いたコンポジット形式でコンテンツデータを提供する場合には、ステップＢ１～Ａ１９の処理を繰り返して各々のセキュアコンテナ１０４を作成し、コンテンツファイルＣＦとキーファイルＫＦとの間のリンク関係と、コンテンツファイルＣＦ相互間のリンク関係とをハイパーリンクなどを用いて結ぶ。

ステップＢ２１：コンテンツプロバイダ１０１は、作成したセキュアコンテナ１０４をセキュアコンテナデータベース１１８ａに格納する。

【０１５８】〔ＥＭＤサービスセンタ１０２〕ＥＭＤサービスセンタ１０２は、認証（ＣＡ：Ｃｅｒｔｉｆｉｃａｔｅ　Ａｕｔｈｏｒｉｔｙ）機能、鍵管理（Ｋｅｙ　Ｍａｎａｇｅｍｅｎｔ）機能および権利処理（Ｒｉｇｈｔｓ　Ｃｌｅａｒｉｎｇ）（利益分配）機能を有する。図２３は、ＥＭＤサービスセンタ１０２の機能の構成図である。図２３に示すように、ＥＭＤサービスセンタ１０２は、鍵サーバ１４１、鍵データベース１４１ａ、決算処理部１４２、署名処理部１４３、決算機関管理部１４４、証明書・権利書管理部１４５、権利書データベース１４５ａ、証明書データベース１４５ｂ、コンテンツプロバイダ管理部１４８、ＣＰデータベース１４８ａ、ＳＡＭ管理部１４９、ＳＡＭデータベース１４９ａ、相互認証部１５０、暗号化・復号部１５１およびＫＦ作成部１５３を有する。なお、図２３には、ＥＭＤサービスセンタ１０２内の機能ブロック相互間のデータの流れのうち、コンテンツプロバイダ１０１との間で送受信されるデータに関連するデータの流れが示されている。また、図２４には、ＥＭＤサービスセンタ１０２内の機能ブロック相互間のデータの流れのうち、ＳＡＭ１０５$_1$～１０５$_4$および図１に示す決済機関９１との間で送受信されるデータに関連するデータの流れが示されている。

【０１５９】鍵サーバ１４１は、鍵データベース１４１ａに記憶された各々有効期間が１カ月の配信用鍵データを要求に応じて６か月分読み出してＳＡＭ管理部１４９に出力する。また、鍵データベース１４１ａ配信用鍵データＫＤの他に、ＥＭＤサービスセンタ１０２の秘密鍵データ$K_{ESC,S}$、記録用鍵データK_{STR}、メディア鍵データK_{MED}およびＭＡＣ鍵データK_{MAC}などの鍵データを記憶する一連の鍵データを格納している。

【０１６０】決算処理部１４２は、ＳＡＭ１０５$_1$～１０５$_4$から入力した利用履歴データ１０８と、証明書・権利書管理部１４５から入力した標準小売価格データＳＲＰおよび販売価格とに基づいて決済処理を行い、決済レポートデータ１０７および決済請求権データ１５２を作成し、決済レポートデータ１０７をコンテンツプロバイダ管理部１４８に出力し、決済請求権データ１５２を決算機関管理部１４４に出力する。なお、決算処理部１４２は、販売価格に基づいて、違法なダンピング価格による取り引きが行われたか否かを監視する。ここで、利用履歴データ１０８は、ユーザホームネットワーク１０３におけるセキュアコンテナ１０４の購入、利用（再生、記録および転送など）の履歴を示し、決算処理部１４２においてセキュアコンテナ１０４に関連したラインセンス料の支払い額を決定する際に用いられる。

【０１６１】利用履歴データ１０８には、例えば、セキュアコンテナ１０４に格納されたコンテンツデータＣの識別子であるコンテンツＩＤ、セキュアコンテナ１０４を配給したコンテンツプロバイダ１０１の識別子ＣＰ＿ＩＤ、セキュアコンテナ１０４内のコンテンツデータＣの圧縮方法、セキュアコンテナ１０４を記録した記録媒体の識別子Ｍｅｄｉａ＿ＩＤ、セキュアコンテナ１０４を配給を受けたＳＡＭ１０５$_1$～１０５$_4$の識別子ＳＡＭ＿ＩＤ、当該ＳＡＭ１０５$_1$～１０５$_4$のユーザのＵＳＥＲ＿ＩＤなどが記述されている。従って、ＥＭＤサービスセンタ１０２は、コンテンツプロバイダ１０１の所有者以外にも、例えば、圧縮方法や記録媒体などのライセンス所有者に、ユーザホームネットワーク１０３のユーザが支払った金銭を分配する必要がある場合には、予め決められた分配率表に基づいて各相手に支払う金額を決定し、当該決定に応じた決済レポートデータ１０７および決済請求権データ１５２を作成する。当該分配率表は、例えば、セキュアコンテナ１０４に格納されたコンテンツデータ毎に作成される。

【０１６２】また、決済請求権データ１５２は、当該データに基づいて、決済機関９１に金銭の支払いを請求できる権威化されたデータであり、例えば、ユーザが支払った金銭を複数の権利者に配給する場合には、個々の権利者毎に作成される。なお、決済機関９１は、決済が終了すると、当該決済機関の利用明細書をＥＭＤサービスセンタ１０２に送る。ＥＭＤサービスセンタ１０２は、当該利用明細書の内容を、対応する権利者に通知する。

【０１６３】決算機関管理部１４４は、決算処理部１４２が生成した決済請求権利データ１５２を図１に示すペイメントゲートウェイ９０を介して決済機関９１に送信するなお、後述するように、決算機関管理部１４４は、決済請求権データ１５２を、コンテンツプロバイダ１０１などの権利者に送信し、受信した決済請求権データ１５２を用いて、権利者自らが決済機関９１に対しての決済を行ってもよい。また、決算機関管理部１４４は、署名処理部１４３において決済請求権データ１５２のハッシュ値をとり、秘密鍵データ$K_{ESC,S}$を用いて生成した署名データSIG_{99}を決済請求権データ１５２と共に決済機関９１に送信する。

【０１６４】証明書・権利書管理部１４５は、証明書データベース１４５ｂに登録（記録）されて権威化された公開鍵証明書データＣＥＲ$_{CP}$および公開鍵証明書データＣＥＲ$_{SAM1}$～ＣＥＲ$_{SAM4}$などを読み出すと共に、コンテンツプロバイダ１０１の権利書データ１０６、コンテンツ鍵データＫｃおよび電子透かし情報管理データＷＭなどを権利書データベース１４５ａに登録して権威化する。ここで、権利書データベース１４５ａはコンテンツＩＤを検索キーとして検索が行われ、証明書データベース１４５ｂはコンテンツプロバイダ１０１の識別子ＣＰ＿ＩＤを検索キーとして検索が行われる。また、証明書・権利書管理部１４５は、例えば、権利書デ

ータ１０６、コンテンツ鍵データＫｃおよび電子透かし情報管理データWMなどのハッシュ値をとり、秘密鍵データ$K_{ESC,S}$を用いた署名データを付した権威化されたデータを権利書データベース１４５ａに格納する。

【０１６５】コンテンツプロバイダ管理部１４８は、コンテンツプロバイダ１０１との間で通信する機能を有し、登録されたコンテンツプロバイダ１０１の識別子ＣＰ＿ＩＤなどを管理するＣＰデータベース１４８ａにアクセスできる。

【０１６６】ＳＡＭ管理部１４９は、ユーザホームネットワーク１０３内のＳＡＭ105_1～105_4との間で通信する機能を有し、登録されたＳＡＭの識別子ＳＡＭ＿ＩＤやＳＡＭ登録リストなどを記録したＳＡＭデータベース１４９ａにアクセスできる。

【０１６７】ＫＦ作成部１５３は、コンテンツプロバイダ管理部１４８から入力したコンテンツ鍵データＫｃおよび権利書データ１０６と、ＳＡＭプログラム・ダウンロード・コンテナSDC_1～SDC_3とを署名処理部１４３に出力する。また、ＫＦ作成部１５３は、鍵サーバ１４１から入力した対応する期間の配信用鍵データKD_1～KD_6を用いて、コンテンツ鍵データＫｃ、権利書データ１０６およびＳＡＭプログラム・ダウンロード・コンテナSDC_1～SDC_3を暗号化し、図５（Ｂ）に示すように、当該暗号化したデータと、署名処理部１４３から入力した当該暗号化したデータについての秘密鍵データ$K_{ESC,S}$による署名データ$SIG_{K1,ESC}$とを格納したキーファイルＫＦを作成し、当該作成したキーファイルＫＦをＫＦデータベース１５３ａに格納する。

【０１６８】以下、ＥＭＤサービスセンタ１０２内での処理の流れを説明する。先ず、ＥＭＤサービスセンタ１０２からユーザホームネットワーク１０３内のＳＡＭ105_1～105_4に配信用鍵データを送信する際の処理の流れを、図２４を参照しながら説明する。図２４に示すように、鍵サーバ１４１は、所定期間毎に、例えば、３カ月分の配信用鍵データKD_1～KD_3を鍵データベース１４１ａから読み出してＳＡＭ管理部１４９に出力する。また、署名処理部１４３は、配信用鍵データKD_1～KD_3の各々のハッシュ値をとり、ＥＭＤサービスセンタ１０２の秘密鍵データ$K_{ESC,S}$を用いて、それぞれに対応する署名データ$SIG_{KD1,ESC}$～$SIG_{KD3,ESC}$を作成し、これをＳＡＭ管理部１４９に出力する。ＳＡＭ管理部１４９は、この３カ月分の配信用鍵データKD_1～KD_3およびそれらの署名データ$SIG_{KD1,ESC}$～$SIG_{KD3,ESC}$を、相互認証部１５０とＳＡＭ105_1～105_4と間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、ＳＡＭ105_1～105_4に送信する。

【０１６９】次に、ＥＭＤサービスセンタ１０２がコンテンツプロバイダ１０１から、公開鍵証明書データCER_{CP}の発行要求を受けた場合の処理を、図２３を参照しながら説明する。この場合に、コンテンツプロバイダ管理部１４８は、コンテンツプロバイダ１０１の識別子ＣＰ＿ＩＤ、公開鍵データ$K_{CP,P}$および署名データ$SIG_{9,CP}$をコンテンツプロバイダ１０１から受信すると、これらを、相互認証部１５０と図４に示す相互認証部１２０と間の相互認証で得られたセッション鍵データK_{SES}を用いて復号する。そして、当該復号した署名データ$SIG_{9,CP}$の正当性を署名処理部１４３において確認した後に、識別子ＣＰ＿ＩＤおよび公開鍵データ$K_{CP,P}$に基づいて、当該公開鍵証明書データの発行要求を出したコンテンツプロバイダ１０１がＣＰデータベース１４８ａに登録されているか否かを確認する。そして、証明書・権利書管理部１４５は、当該コンテンツプロバイダ１０１の公開鍵証明書データCER_{CP}を証明書データベース１４５ｂから読み出してコンテンツプロバイダ管理部１４８に出力する。また、署名処理部１４３は、公開鍵証明書データCER_{CP}のハッシュ値をとり、ＥＭＤサービスセンタ１０２の秘密鍵データ$K_{ESC,S}$を用いて、署名データ$SIG_{1,ESC}$を作成し、これをコンテンツプロバイダ管理部１４８に出力する。そして、コンテンツプロバイダ管理部１４８は、公開鍵証明書データCER_{CP}およびその署名データ$SIG_{1,ESC}$を、相互認証部１５０と図４に示す相互認証部１２０と間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、コンテンツプロバイダ１０１に送信する。

【０１７０】次に、ＥＭＤサービスセンタ１０２がＳＡＭ105_1から、公開鍵証明書データCER_{SAM1}の発行要求を受けた場合の処理を、図２４を参照しながら説明する　この場合に、ＳＡＭ管理部１４９は、ＳＡＭ105_1の識別子SAM_1＿ＩＤ、公開鍵データ$K_{SAM1,P}$および署名データ$SIG_{8,SAM1}$をＳＡＭ105_1から受信すると、これらを、相互認証部１５０とＳＡＭ105_1と間の相互認証で得られたセッション鍵データK_{SES}を用いて復号する。そして、当該復号した署名データ$SIG_{8,SAM1}$の正当性を署名処理部１４３において確認した後に、識別子SAM_1＿ＩＤおよび公開鍵データ$K_{SAM1,P}$に基づいて、当該公開鍵証明書データの発行要求を出したＳＡＭ105_1がＳＡＭデータベース１４９ａに登録されているか否かを確認する。そして、証明書・権利書管理部１４５は、当該ＳＡＭ105_1の公開鍵証明書データCER_{SAM1}を証明書データベース１４５ｂから読み出してＳＡＭ管理部１４９に出力する。また、署名処理部１４３は、公開鍵証明書データCER_{SAM1}のハッシュ値をとり、ＥＭＤサービスセンタ１０２の秘密鍵データ$K_{ESC,S}$を用いて、署名データ$SIG_{50,ESC}$を作成し、これをＳＡＭ管理部１４９に出力する。そして、ＳＡＭ管理部１４９は、公開鍵証明書データＣＥＲ

$_{SAM1}$およびその署名データ$SIG_{50,ESC}$を、相互認証部１５０とSAM１０５$_1$と間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、SAM１０５$_1$に送信する。なお、SAM１０５$_2$～１０５$_4$が、公開鍵証明書データを要求した場合の処理は、対象がSAM１０５$_2$～１０５$_4$に代わるのみで、基本的に上述したSAM１０５$_1$の場合と同じである。なお、本発明では、EMDサービスセンタ１０２は、例えば、SAM１０５$_1$の出荷時に、SAM１０５$_1$の秘密鍵データ$K_{SAM1,S}$および公開鍵データ$K_{SAM1,P}$をSAM１０５$_1$の記憶部に記憶する場合には、当該出荷時に、公開鍵データ$K_{SAM1,P}$の公開鍵証明書データCER_{SAM1}を作成してもよい。このとき、当該出荷時に、公開鍵証明書データCER_{SAM1}を、SAM１０５$_1$の記憶部に記憶してもよい。

【０１７１】次に、EMDサービスセンタ１０２が、コンテンツプロバイダ１０１から図１８に示す登録用モジュールMod$_2$を受けた場合の処理を、図２３を参照しながら説明する。この場合には、コンテンツプロバイダ管理部１４８がコンテンツプロバイダ１０１から図１８に示す登録用モジュールMod$_2$を受信すると、相互認証部１５０と図４に示す相互認証部１２０と間の相互認証で得られたセッション鍵データK_{SES}を用いて登録用モジュールMod$_2$を復号する。そして、署名処理部１４３において、鍵データベース１４１ａから読み出した公開鍵データ$K_{CP,P}$を用いて、署名データ$SIG_{M1,CP}$の正当性を検証する。次に、証明書・権利書管理部１４５は、登録用モジュールMod$_2$に格納された権利書データ１０６、コンテンツ鍵データKc、電子透かし情報管理データWMおよびSRPを、権利書データベース１４５ａに登録する。

【０１７２】次に、コンテンツプロバイダ管理部１４８は、コンテンツ鍵データKcおよび権利書データ１０６をKF作成部１５３に出力する。次に、KF作成部１５３は、コンテンツプロバイダ管理部１４８から入力したコンテンツ鍵データKcおよび権利書データ１０６と、SAMプログラム・ダウンロード・コンテナSDC$_1$～SDC$_3$とを署名処理部１４３に出力する。そして、署名処理部１４３は、KF作成部１５３から入力したデータ全体に対してハッシュ値をとり、EMDサービスセンタ１０２の秘密鍵データ$K_{ESC,S}$を用いて、その署名データ$SIG_{K1,ESC}$を作成し、これをKF作成部１５３に出力する。次に、KF作成部１５３において、鍵サーバ１４１から入力した対応する期間の配信用鍵データKD$_1$～KD$_6$を用いて、コンテンツ鍵データKcおよび権利書データ１０６と、SAMプログラム・ダウンロード・コンテナSDC$_1$～SDC$_3$を暗号化し、当該暗号化したデータと、署名処理部１４３から入力した署名データ$SIG_{K1,ESC}$とを格納したキーファイルKFを作成し、これをKFデータベース１５３ａに格納する。ここで、SAMプログラム・ダウンロード・コンテナSDC$_1$～SDC$_3$は、登録用モジュールMod$_2$内に格納したものを用いても、あるいはEMDサービスセンタ１０２が予め保持しているものを用いてもよい。次に、コンテンツプロバイダ管理部１４８は、KFデータベース１５３ａにアクセスを行って得たキーファイルKFを、相互認証部１５０と図４に示す相互認証部１２０と間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、コンテンツプロバイダ１０１に送信する。

【０１７３】次に、EMDサービスセンタ１０２において行なう決済処理を図２４を参照しながら説明する。SAM管理部１４９は、ユーザホームネットワーク１０３の例えばSAM１０５$_1$から利用履歴データ１０８およびその署名データ$SIG_{200,SAM1}$を入力すると、利用履歴データ１０８および署名データ$SIG_{200,SAM1}$を、相互認証部１５０とSAM１０５$_1$との間の相互認証によって得られたセッション鍵データK_{SES}を用いて復号し、SAM１０５$_1$の公開鍵データK_{SAM1}による署名データ$SIG_{200,SAM1}$の検証を行なった後に、決算処理部１４２に出力する。

【０１７４】そして、決算処理部１４２は、SAM管理部１４９から入力した利用履歴データ１０８と、証明書・権利書管理部１４５を介して権利書データベース１４５ａから読み出した権利書データ１０６に含まれる標準小売価格データSRPおよび販売価格とに基づいて決済処理を行い、決済請求権データ１５２および決済レポートデータ１０７を生成する。決算処理部１４２は、決済請求権データ１５２を決算機関管理部１４４に出力すると共に、決済レポートデータ１０７をコンテンツプロバイダ管理部１４８に出力する。

【０１７５】次に、決算機関管理部１４４は、決済請求権データ１５２およびその署名データSIG_{99}を、相互認証およびセッション鍵データK_{SES}による復号を行なった後に、図１に示すペイメントゲートウェイ９０を介して決済機関９１に送信する。これにより、決済請求権データ１５２に示される金額の金銭が、コンテンツプロバイダ１０１に支払われる。

【０１７６】次に、EMDサービスセンタ１０２がコンテンツプロバイダ１０１に決済レポートを送信する場合の処理を図２３を参照しながら説明する。決算処理部１４２において決済が行なわれると、前述したように、決算処理部１４２からコンテンツプロバイダ管理部１４８に決済レポートデータ１０７が出力される。決済レポートデータ１０７は、上述したように、例えば、EMDサービスセンタ１０２が図１に示す決済機関９１に対して行なったコンテンツプロバイダ１０１に関する決済の内容が記述されている。EMDサービスセンタ１０２は、決算処理部１４２から決済レポートデータ１０７を入力

89

すると、これを、相互認証部１５０と図４に示す相互認証部１２０と間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、コンテンツプロバイダ１０１に送信する。

【０１７７】また、EMDサービスセンタ１０２は、前述したように、権利書データ１０６を登録（権威化）した後に、EMDサービスセンタ１０２からコンテンツプロバイダ１０１に、権威化証明書モジュールを配信用鍵データKD_1～KD_6で暗号化して送信してもよい。

【０１７８】また、EMDサービスセンタ１０２は、その他に、$SAM105_1$～105_4の出荷時の処理と、SAM登録リストの登録処理とを行なうが、これらの処理については後述する。

【０１７９】［ユーザホームネットワーク１０３］ユーザホームネットワーク１０３は、図１に示すように、ネットワーク機器160_1およびA／V機器160_2～160_4を有している。ネットワーク機器160_1は、$SAM105_1$を内蔵している。また、AV機器160_2～160_4は、それぞれ$SAM105_2$～105_4を内蔵している。$SAM105_1$～105_4の相互間は、例えば、IEEE１３９４シリアルインタフェースバスなどのバス１９１を介して接続されている。なお、AV機器160_2～160_4は、ネットワーク通信機能を有していてもよいし、ネットワーク通信機能を有しておらず、バス１９１を介してネットワーク機器160_1のネットワーク通信機能を利用してもよい。また、ユーザホームネットワーク１０３は、ネットワーク機能を有していないAV機器のみを有していてもよい。

【０１８０】以下、ネットワーク機器160_1について説明する。図２５は、ネットワーク機器160_1の構成図である。図２５に示すように、ネットワーク機器160_1は、$SAM105_1$、通信モジュール１６２、復号・伸長モジュール１６３、購入・利用形態決定操作部１６５、ダウンロードメモリ１６７、再生モジュール１６９および外部メモリ２０１を有する。

【０１８１】$SAM105_1$～105_4は、コンテンツ単位の課金処理をおこなうモジュールであり、EMDサービスセンタ１０２との間で通信を行う。$SAM105_1$～105_4は、例えば、EMDサービスセンタ１０２によって仕様およびバージョンなどが管理され、家庭機器メーカに対し、搭載の希望があればコンテンツ単位の課金を行うブラックボックスの課金モジュールとしてライセンス譲渡される。例えば、家庭機器開発メーカは、$SAM105_1$～105_4のIC（Integrated Circuit）の内部の仕様を知ることはできず、EMDサービスセンタ１０２が当該ICのインタフェースなどを統一化し、それに従ってネットワーク機器160_1およびAV機器160_2～160_4に搭載される。

【０１８２】$SAM105_1$～105_4は、その処理内

90

容が外部から完全に遮蔽され、その処理内容を外部から監視および改竄不能であり、また、内部に予め記憶されているデータおよび処理中のデータを外部から監視および改竄不能な耐タンパ（Tamper Registance）性を持ったハードウェアモジュール（ICモジュールなど）である。$SAM105_1$～105_4の機能をICという形で実現する場合は、IC内部に秘密メモリを持ち、そこに秘密プログラムおよび秘密データが格納される。SAMをICという物理的形態にとらわれず、その機能を機器の何れかの部分に組み込むことができれば、その部分をSAMとして定義してもよい。

【０１８３】以下、$SAM105_1$の機能について詳細に説明する。なお、$SAM105_2$～105_4は、$SAM105_1$と基本的に同じ機能を有している。図２６は、$SAM105_1$の機能の構成図である。なお、図２６には、コンテンツプロバイダ１０１からのセキュアコンテナ１０４を入力し、セキュアコンテナ１０４内のキーファイルKFを復号する処理に関連するデータの流れが示されている。図２６に示すように、$SAM105_1$は、相互認証部１７０、暗号化・復号部１７１，１７２，１７３、コンテンツプロバイダ管理部１８０、誤り訂正部１８１、ダウンロードメモリ管理部１８２、セキュアコンテナ復号部１８３、復号・伸長モジュール管理部１８４、EMDサービスセンタ管理部１８５、利用監視部１８６、課金処理部１８７、署名処理部１８９、SAM管理部１９０、メディアSAM管理部１９７、スタック（作業）メモリ２００および外部メモリ管理部８１１を有する。なお、AV機器160_2～160_4はダウンロードメモリ１６７を有していないため、$SAM105_2$～105_4にはダウンロードメモリ管理部１８２は存在しない。

【０１８４】なお、図２６に示す$SAM105_1$の所定の機能は、例えば、図示しないCPUにおいて秘密プログラムを実行することによって実現される。また、外部メモリ２０１には、以下に示す処理を経て、図２７に示すように、利用履歴データ１０８およびSAM登録リストが記憶される。ここで、外部メモリ２０１のメモリ空間は、$SAM105_1$の外部（例えば、ホストCPU８１０）からは見ることはできず、$SAM105_1$のみが外部メモリ２０１の記憶領域に対してのアクセスを管理できる。外部メモリ２０１としては、例えば、フラッシュメモリあるいは強誘電体メモリ（FeRAM）などが用いられる。また、スタックメモリ２００としては、例えばSARAMが用いられ、図２８に示すように、セキュアコンテナ１０４、コンテンツ鍵データK_c、権利書データ（UCP）１０６、記憶部１９２のロック鍵データK_{Loc}、コンテンツプロバイダ１０１の公開鍵証明書$CERcp$、利用制御状態データ（UCS）１６６、およびSAMプログラム・ダウンロード・コンテナSDC_1～SDC_3などが記憶される。

91

【０１８５】以下、ＳＡＭ１０５$_1$の機能のうち、コンテンツプロバイダ１０１からのセキュアコンテナ１０４を入力したときの各機能ブロックの処理内容を図２６を参照しながら説明する。

【０１８６】相互認証部１７０は、ＳＡＭ１０５$_1$がコンテンツプロバイダ１０１およびＥＭＤサービスセンタ１０２との間でオンラインでデータを送受信する際に、コンテンツプロバイダ１０１およびＥＭＤサービスセンタ１０２との間で相互認証を行ってセッション鍵データ（共有鍵）K_{SES}を生成し、これを暗号化・復号部１７１に出力する。セッション鍵データK_{SES}は、相互認証を行う度に新たに生成される。

【０１８７】暗号化・復号部１７１は、コンテンツプロバイダ１０１およびＥＭＤサービスセンタ１０２との間で送受信するデータを、相互認証部１７０が生成したセッション鍵データK_{SES}を用いて暗号化・復号する。

【０１８８】誤り訂正部１８１は、セキュアコンテナ１０４を誤り訂正してダウンロードメモリ管理部１８２に出力する。なお、ユーザホームネットワーク１０３は、セキュアコンテナ１０４が改竄されているか否かを検出する機能を有していてもよい。本実施形態では、誤り訂正部１８１を、ＳＡＭ１０５$_1$に内蔵した場合を例示したが、誤り訂正部１８１の機能を、例えばホストＣＰＵ８１０などのＳＡＭ１０５$_1$の外部に持たせてもよい。

【０１８９】ダウンロードメモリ管理部１８２は、図２５に示すようにダウンロードメモリ１６７が相互認証機能を持つメディアＳＡＭ１６７ａを有している場合には、相互認証部１７０とメディアＳＡＭ１６７ａとの間で相互認証を行った後に、誤り訂正後のセキュアコンテナ１０４を、相互認証によって得られたセッション鍵データK_{SES}を用いて暗号化して図２５に示すダウンロードメモリ１６７に書き込む。ダウンロードメモリ１６７としては、例えば、メモリスティックなどの不揮発性半導体メモリが用いられる。なお、図２９に示すように、ＨＤＤ（Ｈａｒｄ　Ｄｉｓｋ　Ｄｒｉｖｅ）などの相互認証機能を備えていないメモリをダウンロードメモリ２１１として用いる場合には、ダウンロードメモリ２１１内はセキュアではないので、コンテンツファイルＣＦをダウンロードメモリ２１１にダウンロードし、機密性の高いキーファイルＫＦを例えば、図２６に示すスタックメモリ２００にダウンロードする。

【０１９０】セキュアコンテナ復号部１８３は、ダウンロードメモリ管理部１８２から入力したセキュアコンテナ１０４に格納されたキーファイルＫＦ内のコンテンツ鍵データＫｃ、権利書データ１０６およびＳＡＭプログラム・ダウンロード・コンテナSDC_1～SDC_3を、記憶部１９２から読み出した対応する期間の配信用鍵データKD_1～KD_3を用いて復号する。当該復号されたコンテンツ鍵データＫｃ、権利書データ１０６およびＳＡＭプログラム・ダウンロード・コンテナSDC_1～SDC_3は、スタックメモリ２００に書き込まれる。

92

【０１９１】ＥＭＤサービスセンタ管理部１８５は、図１に示すＥＭＤサービスセンタ１０２との間の通信を管理する。

【０１９２】署名処理部１８９は、記憶部１９２から読み出したＥＭＤサービスセンタ１０２の公開鍵データ$K_{ESC,P}$およびコンテンツプロバイダ１０１の公開鍵データ$K_{CP,P}$を用いて、セキュアコンテナ１０４内の署名データの検証を行なう。

【０１９３】記憶部１９２は、ＳＡＭ１０５$_1$の外部から読み出しおよび書き換えできない秘密データとして、図３０に示すように、有効期限付きの複数の配信用鍵データKD_1～KD_3、ＳＡＭ＿ＩＤ、ユーザＩＤ、パスワード、情報参照用ＩＤ、ＳＡＭ登録リスト、記録用鍵データK_{STR}、ルートＣＡの公開鍵データ$K_{R-CA,P}$、ＥＭＤサービスセンタ１０２の公開鍵データ$K_{ESC,P}$、メディア鍵データK_{MED}、ＥＭＤサービスセンタ１０２の公開鍵データ$K_{ESC,P}$、ＳＡＭ１０５$_1$の秘密鍵データ$K_{SAM1,S}$、ＳＡＭ１０５$_1$の公開鍵データ$K_{SAM1,P}$を格納した公開鍵証明書CER_{SAM1}、ＥＭＤサービスセンタ１０２の秘密鍵データ$K_{ESC,S}$を用いた公開鍵証明書CER_{ESC}の署名データSIG_{22}、復号・伸長モジュール１６３との間の相互認証用の元鍵データ（共通鍵暗号化方式を採用した場合）、メディアＳＡＭとの間の相互認証用の元鍵データ（共通鍵暗号化方式を採用した場合）、並びにメディアＳＡＭの公開鍵証明書データCER_{MEDSAM}（公開鍵暗号化方式を採用した場合）を記憶している。また、記憶部１９２には、図２６に示す少なくとも一部の機能を実現するための秘密プログラムが記憶されている。記憶部１９２としては、例えば、フラッシュＥＥＰＲＯＭ（Ｅｌｅｃｔｒｉｃａｌｌｙ　Ｅｒａｓａｂｌｅ　Ｐｒｏｇｒａｍｍａｂｌｅ　ＲＡＭ）が用いられる。

【０１９４】以下、ＥＭＤサービスセンタ１０２から受信した配信用鍵データKD_1～KD_3を記憶部１９２に格納する際のＳＡＭ１０５$_1$内での処理の流れを図２６を参照しながら説明する。この場合には、先ず、相互認証部１７０と図２３に示す相互認証部１５０との間で相互認証が行われる。次に、当該相互認証によって得られたセッション鍵データK_{SES}で暗号化された３カ月分の配信用鍵データKD_1～KD_3およびその署名データ$SIG_{KD1,ESC}$～$SIG_{KD3,ESC}$が、ＥＭＤサービスセンタ１０２からＥＭＤサービスセンタ管理部１８５を介してスタックメモリ８１１に書き込まれる。次に、暗号化・復号部１７１において、セッション鍵データK_{SES}を用いて、配信用鍵データKD_1～KD_3およびその署名データ$SIG_{KD1,ESC}$～$SIG_{KD3,ESC}$が復号される。次に、署名処理部１８９において、スタックメモリ８１１に記憶された署名デ

93

ータＳＩＧKD1，ESC～ＳＩＧKD3，ESCの正当性が確認された後に、配信用鍵データＫＤ1～ＫＤ3が記憶部１９２に書き込まれる。

【０１９５】以下、コンテンツプロバイダ１０１が提供したセキュアコンテナ１０４を入力する際のＳＡＭ１０５1内での処理の流れを図２６を参照しながら説明する。図２６に示すＳＡＭ１０５1の相互認証部１７０と図３に示す相互認証部１２０との間で相互認証が行なわれる。暗号化・復号部１７１は、当該相互認証によって得られたセッション鍵データKSESを用いて、コンテンツプロバイダ管理部１８０を介してコンテンツプロバイダ１０１から供給されたセキュアコンテナ１０４を復号する。

【０１９６】次に、署名処理部１８９は、図５（Ｃ）に示す署名データＳＩＧ1，ESCの検証を行なった後に、図５（Ｃ）に示す公開鍵証明書データＣＥＲCP内に格納されたコンテンツプロバイダ１０１の公開鍵データKCP，Pを用いて、署名データＳＩＧ6，CP，ＳＩＧ7，CPの正当性を検証する。このとき、署名データＳＩＧ6，CPが正当であると検証されたときに、コンテンツファイルＣＦの作成者および送信者の正当性が確認される。また、署名データＳＩＧ7，CPが正当であると検証されたときに、キーファイルＫＦの送信者の正当性が確認される。また、署名処理部１８９は、記憶部１９２から読み出した公開鍵データKESC，Pを用いて、図５（Ｂ）に示すキーファイルＫＦ内の署名データＳＩＧK1，ESCの正当性、すなわちキーファイルＫＦの作成者の正当性およびキーファイルＫＦがＥＭＤサービスセンタ１０２に登録されているか否かの検証を行う。コンテンツプロバイダ管理部１８０は、署名データＳＩＧ6，CP，ＳＩＧ7，CP，ＳＩＧK1，ESCの正当性が確認されると、セキュアコンテナ１０４を誤り訂正部１８１に出力する。

【０１９７】誤り訂正部１８１は、セキュアコンテナ１０４を誤り訂正した後に、ダウンロードメモリ管理部１８２に出力する。ダウンロードメモリ管理部１８２は、相互認証部１７０と図２５に示すメディアＳＡＭ１６７ａとの間で相互認証を行なった後に、セキュアコンテナ１０４をダウンロードメモリ１６７に書き込む。

【０１９８】次に、ダウンロードメモリ管理部１８２は、相互認証部１７０と図２５に示すメディアＳＡＭ１６７ａとの間で相互認証を行なった後に、セキュアコンテナ１０４に格納された図５（Ｂ）に示すキーファイルＫＦをダウンロードメモリ１６７から読み出してセキュアコンテナ復号部１８３に出力する。

【０１９９】そして、セキュアコンテナ復号部１８３において、記憶部１９２から入力した対応する期間の配信用鍵データＫＤ1～ＫＤ3を用いて、図５（Ｂ）に示すキーファイルＫＦ内のコンテンツ鍵データＫｃ、権利書データ１０６およびＳＡＭプログラム・ダウンロード・

94

コンテナＳＤＣ1～ＳＤＣ3が復号される。そして、復号されたコンテンツ鍵データＫｃ、権利書データ１０６およびＳＡＭプログラム・ダウンロード・コンテナＳＤＣ1～ＳＤＣ3がスタックメモリ２００に書き込まれる。

【０２００】以下、ダウンロードメモリ１６７にダウンロードされたコンテンツデータＣを利用・購入する処理に関連する各機能ブロックの処理内容を図３１を参照しながら説明する。

【０２０１】利用監視部１８６は、スタックメモリ２００から権利書データ１０６および利用制御状態データ１６６を読み出し、当該読み出した権利書データ１０６および利用制御状態データ１６６によって許諾された範囲内でコンテンツの購入・利用が行われるように監視する。ここで、権利書データ１０６は、図２６を用いて説明したように、復号後にＫＦに格納されてスタックメモリ２００に記憶されている。また、利用制御状態データ１６６は、後述するように、ユーザによって購入形態が決定されたときに、スタックメモリ２００に記憶される。

【０２０２】課金処理部１８７は、図２５に示す購入・利用形態決定操作部１６５からの操作信号Ｓ１６５に応じた利用履歴データ１０８を作成する。ここで、利用履歴データ１０８は、前述したように、ユーザによるセキュアコンテナ１０４の購入および利用の形態の履歴を記述しており、ＥＭＤサービスセンタ１０２において、セキュアコンテナ１０４の購入に応じた決済処理およびライセンス料の支払いを決定する際に用いられる。

【０２０３】また、課金処理部１８７は、必要に応じて、スタックメモリ２００から読み出した販売価格あるいは標準小売価格データＳＲＰをユーザに通知する。ここで、販売価格および標準小売価格データＳＲＰは、復号後にスタックメモリ２００に記憶された図５（Ｂ）に示すキーファイルＫＦの権利書データ１０６内に格納されている。課金処理部１８７による課金処理は、利用監視部１８６の監視の下、権利書データ１０６が示す使用許諾条件などの権利内容および利用制御状態データ１６６に基づいて行われる。すなわち、ユーザは、当該権利内容などに従った範囲内でコンテンツの購入および利用を行う。

【０２０４】また、課金処理部１８７は、操作信号Ｓ１６５に基づいて、ユーザによって決定されたコンテンツの購入形態を記述した利用制御状態（ＵＣＳ：　ＵｓａｇｅＣｏｎｔｒｏｌ　Ｓｔａｔｕｓ）データ１６６を生成し、これをスタックメモリ２００に書き込む。コンテンツの購入形態としては、例えば、購入者による再生や当該購入者の利用のための複製に制限を加えない買い切りや、再生する度に課金を行なう再生課金などがある。ここで、利用制御状態データ１６６は、ユーザがコンテンツの購入形態を決定したときに生成され、以後、当該

95

決定された購入形態で許諾された範囲内でユーザが当該コンテンツの利用を行なうように制御するために用いられる。利用制御状態データ１６６には、コンテンツのＩＤ、購入形態、当該購入形態に応じた価格、当該コンテンツの購入が行なわれたＳＡＭのＳＡＭ＿ＩＤ，購入を行なったユーザのＵＳＥＲ＿ＩＤなどが記述されている。

【０２０５】なお、決定された購入形態が再生課金である場合には、例えば、ＳＡＭ１０５$_1$からコンテンツプロバイダ１０１に利用制御状態データ１６６をコンテンツデータＣの購入と同時にリアルタイムに送信し、コンテンツプロバイダ１０１がＥＭＤサービスセンタ１０２に、利用履歴データ１０８を所定の期間内にＳＡＭ１０５$_1$に取りにいくことを指示する。また、決定された購入形態が買い切りである場合には、例えば、利用制御状態データ１６６が、コンテンツプロバイダ１０１およびＥＭＤサービスセンタ１０２の双方にリアルタイムに送信される。このように、本実施形態では、何れの場合にも、利用制御状態データ１６６をコンテンツプロバイダ１０１にリアルタイムに送信する。

【０２０６】ＥＭＤサービスセンタ管理部１８５は、外部メモリ管理部８１１を介して外部メモリ２０１から読み出した利用履歴データ１０８をＥＭＤサービスセンタ１０２に送信する。このとき、ＥＭＤサービスセンタ管理部１８５は、署名処理部１８９において、秘密鍵データ$K_{SAM1,s}$を用いて利用履歴データ１０８の署名データ$SIG_{200,SAM1}$を作成し、署名データ$SIG_{200,SAM1}$を利用履歴データ１０８と共にＥＭＤサービスセンタ１０２に送信する。ＥＭＤサービスセンタ１０２への利用履歴データ１０８の送信は、例えば、ＥＭＤサービスセンタ１０２からの要求に応じてあるいは定期的に行ってもよいし、利用履歴データ１０８に含まれる履歴情報の情報量が所定以上になったときに行ってもよい。当該情報量は、例えば、外部メモリ２０１の記憶容量に応じて決定される。

【０２０７】ダウンロードメモリ管理部１８２は、例えば、図２５に示す購入形態決定操作部１６５からの操作信号Ｓ１６５に応じてコンテンツの再生動作が行われる場合に、ダウンロードメモリ１６７から読み出したコンテンツデータＣ、スタックメモリ２００から読み出したコンテンツ鍵データＫｃおよび課金処理部１８７から入力したユーザ電子透かし情報用データ１９６を復号・伸長モジュール管理部１８４に出力する。また、復号・伸長モジュール管理部１８４は、図２５に示す購入形態決定操作部１６５からの操作信号Ｓ１６５に応じてコンテンツの試聴動作が行われる場合に、ダウンロードメモリ１６７から読み出したコンテンツファイルＣＦ、並びにスタックメモリ２００から読み出したコンテンツ鍵データＫｃおよび半開示パラメータデータ１９９を復号・伸長モジュール管理部１８４に出力する。

96

【０２０８】ここで、半開示パラメータデータ１９９は、権利書データ１０６内に記述されており、試聴モード時のコンテンツの取り扱いを示している。復号・伸長モジュール１６３では、半開示パラメータデータ１９９に基づいて、暗号化されたコンテンツデータＣを、半開示状態で再生することが可能になる。半開示の手法としては、例えば、復号・伸長モジュール１６３がデータ（信号）を所定のブロックを単位として処理することを利用して、半開示パラメータデータ１９９によって、コンテンツ鍵データＫｃを用いて復号を行うブロックと復号を行わないブロックとを指定したり、試聴時の再生機能を限定したり、試聴可能な期間を限定するものなどがある。

【０２０９】以下、ＳＡＭ１０５$_1$内での処理の流れについて説明する。先ず、コンテンツプロバイダ１０１からダウンロードメモリ１６７にダウンロードされたセキュアコンテナ１０４の購入形態を決定するまでの処理の流れを図３１を参照しながら説明する。ユーザによる図２５に示す購入・利用形態決定操作部１６５の操作によって、試聴モードを示す操作信号Ｓ１６５が課金処理部１８７に出力されると、例えば、ダウンロードメモリ１６７に記憶されているコンテンツファイルＣＦが、復号・伸長モジュール管理部１８４を介して、図２５に示す復号・伸長モジュール１６３に出力される。このとき、コンテンツファイルＣＦに対して、相互認証部１７０とメディアＳＡＭ１６７ａとの間の相互認証およびセッション鍵データK_{SES}による暗号化・復号と、相互認証部１７０と相互認証部２２０との間の相互認証およびセッション鍵データK_{SES}による暗号化・復号とが行なわれる。コンテンツファイルＣＦは、図２５に示す復号部２２１においてセッション鍵データK_{SES}を用いて復号された後に、復号部２２２に出力される。

【０２１０】また、スタックメモリ２００から読み出されたコンテンツ鍵データＫｃおよび半開示パラメータデータ１９９が、図２５に示す復号・伸長モジュール１６３に出力される。このとき、相互認証部１７０と相互認証部２２０との間の相互認証後に、コンテンツ鍵データＫｃおよび半開示パラメータデータ１９９に対してセッション鍵データK_{SES}による暗号化および復号が行なわれる。次に、復号された半開示パラメータデータ１９９が半開示処理部２２５に出力され、半開示処理部２２５からの制御によって、復号部２２２によるコンテンツ鍵データＫｃを用いたコンテンツデータＣの復号が半開示で行われる。次に、半開示で復号されたコンテンツデータＣが、伸長部２２３において伸長された後に、電子透かし情報処理部２２４に出力される。次に、電子透かし情報処理部２２４においてユーザ電子透かし情報用データ１９６がコンテンツデータＣに埋め込まれた後、コンテンツデータＣが再生モジュール１６９において再生され、コンテンツデータＣに応じた音響が出力される。

【０２１１】そして、コンテンツを試聴したユーザが、購入・利用形態決定操作部１６５を操作して購入形態を決定すると、当該決定した購入形態を示す操作信号Ｓ１６５が課金処理部１８７に出力される。そして、課金処理部１８７において、決定された購入形態に応じた利用履歴データ１０８および利用制御状態データ１６６が生成され、利用履歴データ１０８が外部メモリ管理部８１を介して外部メモリ２０１に書き込まれると共に、利用制御状態データ１６６がスタックメモリ２００に書き込まれる。以後は、利用監視部１８６において、利用制御状態データ１６６によって許諾された範囲で、コンテンツの購入および利用が行なわれるように制御（監視）される。

【０２１２】そして、後述する図３４（Ｃ）に示す新たなキーファイルKF_1が作成され、当該作成されたキーファイルKF_1がダウンロードメモリ管理部１８２を介してダウンロードメモリ１６７に記憶される。図３４（Ｃ）に示すように、キーファイルKF_1に格納された利用制御状態データ１６６はストレージ鍵データK_{STR}および メディア鍵データK_{MED}を用いてＤＥＳのＣＢＣモードを利用して順に暗号化されている。ここで、記録用鍵データK_{STR}は、例えばＳＡＣＤ（Ｓｕｐｅｒ Ａｕｄｉｏ Ｃｏｍｐａｃｔ Ｄｉｓｃ）、ＤＶＤ（Ｄｉｇｉｔａｌ Ｖｅｒｓａｔｉｌｅ Ｄｉｓｃ）機器、ＣＤ－Ｒ機器およびＭＤ（Ｍｉｎｉ Ｄｉｓｃ）機器などの種類に応じて決まるデータであり、機器の種類と記録媒体の種類とを１対１で対応づけるために用いられる。また、メディア鍵データK_{MED}は、記録媒体にユニークなデータである。

【０２１３】また、署名処理部１８９において、ＳＡＭ105_1の秘密鍵データ$K_{SAM1,S}$を用いて、キーファイルKF_1のハッシュ値H_{K1}が作成され、当該作成されたハッシュ値H_{K1}が、キーファイルKF_1と対応付けられてスタックメモリ２００に書き込まれる。ハッシュ値H_{K1}は、キーファイルKF_1の作成者の正当性およびキーファイルKF_1が改竄されたか否かを検証するために用いられる。

【０２１４】次に、ダウンロードメモリ１６７に記憶されている購入形態が既に決定されたコンテンツデータＣを再生する場合の処理の流れを、図３１を参照しながら説明する。この場合には、利用監視部１８６の監視下で、操作信号Ｓ１６５に基づいて、ダウンロードメモリ１６７に記憶されているコンテンツファイルＣＦが、図３１に示す復号・伸長モジュール１６３に出力される。このとき、図３１に示す相互認証部１７０と、図２５に示す復号・伸長モジュール１６３の相互認証部２２０との間で相互認証が行われる。また、スタックメモリ２００から読み出されたコンテンツ鍵データＫｃが復号・伸長モジュール１６３に出力される。そして、復号・伸長モジュール１６３の復号部２２２において、コンテンツ鍵データＫｃを用いたコンテンツファイルＣＦの復号と、伸長部２２３による伸長処理とが行なわれ、再生モジュール１６９において、コンテンツデータＣが再生される。このとき、課金処理部１８７によって、操作信号Ｓ１６５に応じて、外部メモリ２０１に記憶されている利用履歴データ１０８が更新される。利用履歴データ１０８は、外部メモリ２０１から読み出された後、相互認証を経て、ＥＭＤサービスセンタ管理部１８５を介して、署名データ$SIG_{200,SAM1}$と共にＥＭＤサービスセンタ１０２に送信される。

【０２１５】次に、図３２に示すように、例えば、前述したようにネットワーク機器1601_1のダウンロードメモリ１６７にダウンロードされたコンテンツファイルＣＦの購入形態を決定した後に、当該コンテンツファイルＣＦを格納した新たなセキュアコンテナ１０４ｘを生成し、バス１９１を介して、ＡＶ機器1602_2のＳＡＭ1052_2にセキュアコンテナ１０４ｘを転送する場合のＳＡＭ1051_1内での処理の流れを図３３を参照しながら説明する。ユーザは、購入・利用形態決定操作部１６５を操作して、ダウンロードメモリ１６７に記憶された所定のコンテンツをＡＶ機器1602_2に転送することを指示し、当該操作に応じた操作信号Ｓ１６５が、課金処理部１８７に出力される。これにより、課金処理部１８７は、操作信号Ｓ１６５に基づいて、外部メモリ２０１に記憶されている利用履歴データ１０８を更新する。また、課金処理部１８７は、コンテンツデータの購入形態が決定される度に、当該決定された購入形態を示す利用制御状態データ１６６をＥＭＤサービスセンタ管理部１８５を介してＥＭＤサービスセンタ１０２に送信する。

【０２１６】また、ダウンロードメモリ管理部１８２は、ダウンロードメモリ１６７から読み出した図５（Ａ）に示すコンテンツファイルＣＦおよびその署名データ$SIG_{6,CP}$と、キーファイルＫＦおよびその署名データ$SIG_{7,CP}$と、キーファイルKF_1およびそのハッシュ値H_{K1}とをＳＡＭ管理部１９０に出力する。このとき、ＳＡＭ1051_1の相互認証部１７０とメディアＳＡＭ１６７ａとの間の相互認証およびセッション鍵データK_{SES}による暗号化・復号が行われる。また、署名処理部１８９は、コンテンツファイルＣＦのハッシュ値をとり、秘密鍵データ$K_{SAM1,S}$を用いて署名データ$SIG_{41,SAM1}$を作成し、これをＳＡＭ管理部１９０に出力する。また、署名処理部１８９は、キーファイルKF_1のハッシュ値をとり、秘密鍵データ$K_{SAM1,S}$を用いて署名データ$SIG_{42,SAM1}$を作成し、これをＳＡＭ管理部１９０に出力する。また、ＳＡＭ管理部１９０は、記憶部１９２から、図３４（Ｄ）に示す公開鍵証明書データCER_{CP}およびその署名データ$SIG_{1,ESC}$と、公開鍵証明書データCER_{SAM1}およびその署名データ$SIG_{22,ESC}$とを読み出す。

99

【０２１７】また、相互認証部１７０は、ＳＡＭ１０５$_2$との間で相互認証を行って得たセッション鍵データＫ$_{SES}$を暗号化・復号部１７１に出力する。ＳＡＭ管理部１９０は、図３４（Ａ），（Ｂ），（Ｃ），（Ｄ）に示すデータからなる新たなセキュアコンテナ１０４ｘを生成し、暗号化・復号部１７１において、セッション鍵データＫ$_{SES}$を用いてセキュアコンテナ１０４ｘを暗号化した後に、図３２に示すＡＶ機器１６０$_2$のＳＡＭ１０５$_2$に出力する。このとき、ＳＡＭ１０５$_1$とＳＡＭ１０５$_2$との間の相互認証と並行して、ＩＥＥＥ１３９４シリアルバスであるバス１９１の相互認証が行われる。

【０２１８】以下、図３２に示すように、ＳＡＭ１０５$_1$から入力したセキュアコンテナ１０４ｘを、ＲＡＭ型などの記録媒体（メディア）１３０$_4$に書き込む際のＳＡＭ１０５$_2$内での処理の流れを、図３５を参照しながら説明する。ここで、ＲＡＭ型の記録媒体１３０$_4$は、例えば、セキュアでないＲＡＭ領域１３４、メディアＳＡＭ１３３およびセキュアＲＡＭ領域１３２を有している。

【０２１９】この場合には、ＳＡＭ１０５$_2$のＳＡＭ管理部１９０は、図３２および図３５に示すように、ネットワーク機器１６０$_1$のＳＡＭ１０５$_1$からセキュアコンテナ１０４ｘを入力する。そして、暗号化・復号部１７１において、ＳＡＭ管理部１９０を介して入力したセキュアコンテナ１０４ｘが、相互認証部１７０とＳＡＭ１０５$_1$の相互認証部１７０との間の相互認証によって得られたセッション鍵データＫ$_{SES}$を用いて復号される。

【０２２０】次に、署名処理部１８９において、公開鍵データＫ$_{CP,\ P}$を用いて、署名データＳＩＧ$_{6,\ CP}$の正当性が検証され、コンテンツファイルＣＦの作成者の正当性が確認される。また、署名処理部１８９において、公開鍵データＫ$_{SAM1,\ P}$を用いて、署名データＳＩＧ$_{41,\ SAM1}$の正当性が検証され、コンテンツファイルＣＦの送信者の正当性が確認される。そして、コンテンツファイルＣＦの作成者および送信者が正当であると確認された後に、ＳＡＭ管理部１９０から記録モジュール管理部８５５にコンテンツファイルＣＦが出力され、コンテンツファイルＣＦが図３２に示すＲＡＭ型の記録媒体１３０$_4$のＲＡＭ領域１３４に書き込まれる。

【０２２１】また、セッション鍵データＫ$_{SES}$を用いて復号されたキーファイルＫＦおよびその署名データＳＩＧ$_{7,\ CP}$，ＳＩＧ$_{42,\ SAM1}$と、キーファイルＫＦ$_1$およびそのハッシュ値Ｈ$_{K1}$と、公開鍵署名データＣＥＲ$_{CP}$およびその署名データＳＩＧ$_{1,\ ESC}$と、公開鍵署名データＣＥＲ$_{SAM1}$およびその署名データＳＩＧ$_{22,\ ESC}$とが、スタックメモリ２００に書き込まれる。

100

【０２２２】次に、署名処理部１８９は、スタックメモリ２００から読み出した署名データＳＩＧ$_{22,\ ESC}$を、記憶部１９２から読み出した公開鍵データＫ$_{ESC,\ P}$を用いて検証して、公開鍵証明書データＣＥＲ$_{SAM1}$の正当性を確認する。そして、署名処理部１８９は、公開鍵証明書データＣＥＲ$_{SAM1}$の正当性を確認すると、公開鍵証明書データＣＥＲ$_{SAM1}$に格納された公開鍵データＫ$_{SAM1,\ P}$を用いて、スタックメモリ２００に記憶されている署名データＳＩＧ$_{42,\ SAM1}$の正当性を検証する。そして、署名データＳＩＧ$_{42,\ SAM1}$が正当であると検証されたときに、キーファイルＫＦの送信者の正当性が確認される。また、署名処理部１８９は、スタックメモリ２００から読み出した署名データＳＩＧ$_{1,\ ESC}$を、記憶部１９２から読み出した公開鍵データＫ$_{ESC,\ P}$を用いて検証して、公開鍵証明書データＣＥＲ$_{CP}$の正当性を確認する。そして、署名処理部１８９は、公開鍵証明書データＣＥＲ$_{CP}$の正当性を確認すると、公開鍵証明書データＣＥＲ$_{CP}$に格納された公開鍵データＫ$_{CP,\ P}$を用いて、スタックメモリ２００に記憶されている署名データＳＩＧ$_{7,\ SAM1}$の正当性を検証する。そして、署名データＳＩＧ$_{7,\ SAM1}$が正当であると検証されたときに、キーファイルＫＦの作成者の正当性が確認される。キーファイルＫＦの作成者および送信者が正当であることが確認されると、キーファイルＫＦがスタックメモリ２００から読み出され、記録モジュール管理部８５５を介して、図３４に示すＲＡＭ型の記録媒体１３０$_4$のセキュアＲＡＭ領域１３２に書き込まれる。

【０２２３】また、署名処理部１８９は、公開鍵データＫ$_{SAM1,\ P}$を用いて、ハッシュ値Ｈ$_{K1}$の正当性を検証し、キーファイルＫＦ$_1$の作成者および送信者の正当性を確認する。そして、キーファイルＫＦ$_1$の作成者および送信者の正当性が確認されると、図３４（Ｃ）に示すキーファイルＫＦ$_1$をスタックメモリ２００から読み出して暗号化・復号部１７３に出力する。なお、当該例では、キーファイルＫＦ$_1$の作成者と送信元とが同じ場合を述べたが、キーファイルＫＦ$_1$の作成者と送信元とが異なる場合には、キーファイルＫＦ$_1$に対して作成者の署名データと送信者と署名データとが作成され、署名処理部１８９において、双方の署名データの正当性が検証される。

【０２２４】そして、暗号化・復号部１７３は、記憶部１９２から読み出した記録用鍵データＫ$_{STR}$、メディア鍵データＫ$_{MED}$および購入者鍵データＫ$_{PIN}$を順に用いてキーファイルＫＦ$_1$内のコンテンツ鍵データＫｃおよび利用制御状態データ１６６を暗号化して記録モジュール管理部８５５に出力する。そして、記録モジュール管理部８５５によって、暗号化されたキーファイルＫＦ$_1$が、ＲＡＭ型の記録媒体１３０$_4$のセキュアＲＡＭ領域１３２に記録されるなお、メディア鍵データＫ

101

K_{MED}は、図３３に示す相互認証部１７０と図３２に示すＲＡＭ型の記録媒体１３０_4のメディアＳＡＭ１３３との間の相互認証によって記憶部１９２に事前に記憶されている。

【０２２５】ここで、記録用鍵データK_{STR}は、例えばＳＡＣＤ（Ｓｕｐｅｒ　Ａｕｄｉｏ　Ｃｏｍｐａｃｔ　Ｄｉｓｃ）、ＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｃ）機器、ＣＤ－Ｒ機器およびＭＤ（Ｍｉｎｉ　Ｄｉｓｃ）機器などの種類（当該例では、ＡＶ機器１６０_2）に応じて決まるデータであり、機器の種類と記録媒体の種類とを１対１で対応づけるために用いられる。なお、ＳＡＣＤとＤＶＤとでは、ディスク媒体の物理的な構造が同じであるため、ＤＶＤ機器を用いてＳＡＣＤの記録媒体の記録・再生を行うことができる場合がある。記録用鍵データK_{STR}は、このような場合において、不正コピーを防止する役割を果たす。なお、本実施形態では、記録用鍵データK_{STR}を用いた暗号化を行わないようにしてもよい。

【０２２６】また、メディア鍵データK_{MED}は、記録媒体（当該例では、ＲＡＭ型の記録媒体１３０_4）にユニークなデータである。メディア鍵データK_{MED}は、記録媒体（当該例では、図３２に示すＲＡＭ型の記録媒体１３０_4）側に格納されており、記録媒体のメディアＳＡＭにおいてメディア鍵データK_{MED}を用いた暗号化および復号を行うことがセキュリティの観点から好ましい。このとき、メディア鍵データK_{MED}は、記録媒体にメディアＳＡＭが搭載されている場合には、当該メディアＳＡＭ内に記憶されており、記録媒体にメディアＳＡＭが搭載されていない場合には、例えば、ＲＡＭ領域内のホストＣＰＵ８１０の管理外の領域に記憶されている。なお、本実施形態のように、機器側のＳＡＭ（当該例では、$ＳＡＭ１０５_2$）とメディアＳＡＭ（当該例では、メディアＳＡＭ１３３）との間で相互認証を行い、セキュアな通信経路を介してメディア鍵データK_{MED}を機器側のＳＡＭに転送し、機器側のＳＡＭにおいてメディア鍵データK_{MED}を用いた暗号化および復号を行なってもよい。本実施形態では、記録用鍵データK_{STR}およびメディア鍵データK_{MED}が、記録媒体の物理層のレベルのセキュリティを保護するために用いられる。

【０２２７】また、購入者鍵データK_{PIN}は、コンテンツファイルＣＦの購入者を示すデータであり、例えば、コンテンツを買い切りで購入したときに、当該購入したユーザに対してＥＭＤサービスセンタ１０２によって割り当てられる。購入者鍵データK_{PIN}は、ＥＭＤサービスセンタ１０２において管理される。

【０２２８】また、上述した実施形態では、記録モジュール２６０を用いて、キーファイルＫＦ，$ＫＦ_1$をＲＡＭ型の記録媒体１３０_4のセキュアＲＡＭ領域１３２に記録する場合を例示したが、図３２において点線で示す

102

ように、$ＳＡＭ１０５_2$からメディアＳＡＭ１３３にキーファイルＫＦ，$ＫＦ_1$を記録するようにしてもよい。

【０２２９】次に、コンテンツの購入形態が未決定の図１２に示すＲＯＭ型の記録媒体１３０_1をユーザホームネットワーク３０３がオフラインで配給を受けた場合に、ＡＶ機器１６０_2において購入形態を決定する際の処理の流れを図３６および図３７を参照しながら説明する。ＡＶ機器１６０_2の$ＳＡＭ１０５_2$は、先ず、図３７に示す相互認証部１７０と図１２に示すＲＯＭ型の記録媒体１３０_1のメディアＳＡＭ１３３との間で相互認証を行った後に、メディアＳＡＭ１３３からメディア鍵データK_{MED}を入力する。なお、$ＳＡＭ１０５_2$が、事前にメディア鍵データK_{MED}を保持している場合には、当該入力を行わなくても良い。次に、ＲＯＭ型の記録媒体１３０_1のセキュアＲＡＭ領域１３２に記録されているセキュアコンテナ１０４に格納された図５（Ｂ），（Ｃ）に示すキーファイルＫＦおよびその署名データ$ＳＩＧ_{7,CP}$と、公開鍵証明書データ$ＣＥＲ_{CP}$およびその署名データ$ＳＩＧ_{1,ESC}$とを、メディアＳＡＭ管理部１９７あるいは図示しない読み出しモジュール管理部を介して入力し、これをスタックメモリ２００に書き込む。

【０２３０】次に、署名処理部１８９において、署名データ$ＳＩＧ_{1,ESC}$の正当性を確認した後に、公開鍵証明書データ$ＣＥＲ_{CP}$から公開鍵データ$K_{CP,P}$を取り出し、この公開鍵データ$K_{CP,P}$を用いて、署名データ$ＳＩＧ_{7,CP}$の正当性、すなわちキーファイルＫＦの送信者の正当性を検証する。また、署名処理部１８９において、記憶部１９２から読み出した公開鍵データ$K_{ESC,P}$を用いて、キーファイルＫＦに格納された署名データ$ＳＩＧ_{K1,ESC}$の正当性、すなわちキーファイルＫＦの作成者の正当性を検証する。

【０２３１】署名処理部１８９において署名データ$ＳＩＧ_{7,CP}$，$ＳＩＧ_{K1,ESC}$の正当性が確認されると、スタックメモリ２００からセキュアコンテナ復号部１８３に、キーファイルＫＦを読み出す。次に、セキュアコンテナ復号部１８３において、対応する期間の配信用鍵データ$ＫＤ_1$～$ＫＤ_3$を用いて、キーファイルＫＦに格納されたコンテンツ鍵データＫｃ、権利書データ１０６およびＳＡＭプログラム・ダウンロード・コンテナ$ＳＤＣ_1$～$ＳＤＣ_3$が復号され、これらがスタックメモリ２００に書き込まれる。

【０２３２】次に、図３７に示す相互認証部１７０と図３６に示す復号・伸長モジュール１６３との間で相互認証を行った後に、$ＳＡＭ１０５_2$の復号・伸長モジュール管理部１８４は、スタックメモリ２００に記憶されているコンテンツ鍵データＫｃおよび権利書データ１０６に格納された半開示パラメータデータ１９９、並びにＲＯＭ型の記録媒体１３０_1のＲＯＭ領域１３１から読み出したコンテンツファイルＣＦに格納されたコンテンツ

データＣを図３６に示す復号・伸長モジュール１６３に出力する。次に、復号・伸長モジュール１６３において、コンテンツデータＣがコンテンツ鍵データＫｃを用いて半開示モードで復号された後に伸長され、再生モジュール２７０に出力される。そして、再生モジュール２７０において、復号・伸長モジュール１６３からのコンテンツデータＣが再生される。

【０２３３】次に、ユーザによる図３６に示す購入形態決定操作部１６５の購入操作によってコンテンツの購入形態が決定され、当該決定された購入形態を示す操作信号Ｓ１６５が課金処理部１８７に入力される。

【０２３４】次に、課金処理部１８７は、操作信号Ｓ１６５に応じた利用制御状態データ１６６を作成し、これをスタックメモリ２００に書き込む。次に、スタックメモリ２００から暗号化・復号部１７３に、コンテンツ鍵データＫｃおよび利用制御状態データ１６６が出力される。

【０２３５】次に、暗号化・復号部１７３は、スタックメモリ２００から入力したコンテンツ鍵データＫｃおよび利用制御状態データ１６６を、記憶部１９２から読み出した記録用鍵データK_{STR}、メディア鍵データK_{MED}および購入者鍵データK_{PIN}を用いて順次に暗号化してスタックメモリ２００に書き込む。

【０２３６】次に、メディアＳＡＭ管理部１９７において、スタックメモリ２００から読み出した、暗号化されたコンテンツ鍵データＫｃおよび利用制御状態データ１６６と、ＳＡＭプログラム・ダウンロード・コンテナSDC_1～SDC_3を用いて図３４（Ｃ）に示すキーファイルKF_1が生成される。また、署名処理部１８９において、図３４（Ｃ）に示すキーファイルKF_1のハッシュ値H_{K1}が生成され、当該ハッシュ値H_{K1}がメディアＳＡＭ管理部１９７に出力される。次に、図３７に示す相互認証部１７０と図３６に示すメディアＳＡＭ１３３との間で相互認証を行った後に、メディアＳＡＭ管理部１９７は、キーファイルKF_1およびハッシュ値H_{K1}を、図３６に示す記録モジュール２７１を介してＲＯＭ型の記録媒体130_1のセキュアＲＡＭ領域１３２に書き込む。これにより、購入形態が決定されたＲＯＭ型の記録媒体130_1が得られる。このとき、課金処理部１８７が生成した利用制御状態データ１６６および利用履歴データ１０８は、所定のタイミングで、スタックメモリ２００および外部メモリ２０１からそれぞれ読み出しされたＥＭＤサービスセンタ１０２に送信される。なお、ＲＯＭ型の記録媒体130_1のメディアＳＡＭ１３３にキーファイルＫＦが格納されている場合には、図３６において点線で示されるように、$SAM105_2$はメディアＳＡＭ１３３からキーファイルＫＦを入力する。また、この場合に、$SAM105_2$は、作成したキーファイルKF_1をメディアＳＡＭ１３３に書き込む。

【０２３７】以下、図３８に示すように、ＡＶ機器160_3において購入形態が未決定のＲＯＭ型の記録媒体130_1からセキュアコンテナ１０４を読み出して新たなセキュアコンテナ１０４ｙを生成し、これをＡＶ機器160_2に転送し、ＡＶ機器160_2において購入形態を決定してＲＡＭ型の記録媒体130_5に書き込む際の処理の流れを図３９，図４０を参照しながら説明する。なお、ＲＯＭ型の記録媒体130_1からＲＡＭ型の記録媒体130_5へのセキュアコンテナ１０４の転送は、図１に示すネットワーク機器160_1およびＡＶ機器160_1～160_4のいずれの間で行ってもよい。

【０２３８】先ず、ＡＶ機器160_3のＳＡＭ105_3とＲＯＭ型の記録媒体130_1のメディアＳＡＭ１３３との間で相互認証を行い、ＲＯＭ型の記録媒体130_1のメディア鍵データK_{MED1}をＳＡＭ105_3に転送する。また、ＡＶ機器160_2のＳＡＭ105_2とＲＡＭ型の記録媒体130_5のメディアＳＡＭ１３３との間で相互認証を行い、ＲＡＭ型の記録媒体130_5メディア鍵データK_{MED2}をＳＡＭ105_2に転送する。なお、メディア鍵データK_{MED1}，K_{MED2}を用いた暗号化をメディアＳＡＭ１３３およびメディアＳＡＭ１３３において行う場合には、メディア鍵データK_{MED1}，K_{MED2}の転送は行わない。

【０２３９】次に、$SAM105_3$は、図３９に示すように、メディアＳＡＭ管理部１９７あるいは図示しない読み出しモジュール管理部を介して、ＲＯＭ型の記録媒体130_1のＲＯＭ領域１３１から読み出した図５（Ａ）に示すコンテンツファイルＣＦおよびその署名データ$SIG_{5,CP}$と、セキュアＲＡＭ領域１３２から読み出した図５（Ｂ），（Ｃ）に示すキーファイルＫＦおよびその署名データ$SIG_{7,CP}$と、公開鍵証明書データCER_{CP}およびその署名データ$SIG_{1,ESC}$とを、暗号化・復号部１７１に出力する。また、メディアＳＡＭ管理部１９７から署名処理部１８９に、コンテンツファイルＣＦおよびキーファイルＫＦが出力される。そして、署名処理部１８９において、コンテンツファイルＣＦおよびキーファイルＫＦのハッシュ値がとられ、秘密鍵データ$K_{SAM3,S}$を用いて、それぞれ署名データ$SIG_{350,SAM3}$，$SIG_{352,SAM3}$が生成され、これらが暗号化・復号部１７１に出力される。また、公開鍵証明書データCER_{SAM3}およびその署名データ$SIG_{351,ESC}$が記憶部１９２から読み出されて暗号化・復号部１７１に出力される。

【０２４０】そして、図４０に示すセキュアコンテナ１０４ｙが、暗号化・復号部１７１において$SAM105_3$と105_2との間の相互認証によって得られたセッション鍵データK_{SES}を用いて暗号化された後に、ＳＡＭ管理部１９０を介して、ＡＶ機器160_2のＳＡＭ105_2に出力される。

【０２４１】$SAM105_2$では、図４１に示すよう

105

に、ＳＡＭ管理部１９０を介してＳＡＭ１０５$_3$から入力した図４０に示すセキュアコンテナ１０４ｙを暗号化・復号部１７１においてセッション鍵データＫ$_{SES}$を用いて復号した後に、セキュアコンテナ１０４ｙ内に格納された署名データＳＩＧ$_{6,CP}$，ＳＩＧ$_{350,SAM3}$の正当性、すなわちコンテンツファイルＣＦの作成者および送信者の正当性を確認する。そして、コンテンツファイルＣＦの作成者および送信者が正当であると確認された後に、メディアＳＡＭ管理部１９７を介してＲＡＭ型の記録媒体１３０$_5$のＲＡＭ領域１３４にコンテンツファイルＣＦが書き込まれる。

【０２４２】また、ＳＡＭ管理部１９０を介してＳＡＭ１０５$_3$から入力されたキーファイルＫＦおよびその署名データＳＩＧ$_{7,CP}$、ＳＩＧ$_{350,SAM3}$と、公開鍵証明書データＣＥＲ$_{SAM3}$およびその署名データＳＩＧ$_{351,ESC}$とが、スタックメモリ２００に書き込まれた後に、暗号化・復号部１７１においてセッション鍵データＫ$_{SES}$を用いて復号される。次に、当該復号された署名データＳＩＧ$_{351,ECS}$が、署名処理部１８９において署名検証され、公開鍵証明書データＣＥＲ$_{SAM3}$の正当性が確認されると、公開鍵証明書データＣＥＲ$_{SAM3}$に格納された公開鍵データＫ$_{SAM3}$を用いて、署名データＳＩＧ$_{7,CP}$，ＳＩＧ$_{352,SAM3}$の正当性、すなわちキーファイルＫＦの作成者および送信者の正当性が確認される。そして、キーファイルＫＦの作成者および送信者の正当性が確認されると、スタックメモリ２００からキーファイルＫＦが読み出されてセキュアコンテナ復号部１８３に出力される。

【０２４３】次に、セキュアコンテナ復号部１８３は、対応する期間の配信用鍵データＫＤ$_1$～ＫＤ$_8$を用いて、キーファイルＫＦを復号し、当該復号したキーファイルＫＦをスタックメモリ２００に書き込む。

【０２４４】次に、スタックメモリ２００に記憶されている既に復号されたキーファイルＫＦに格納された権利書データ１０６が、利用監視部１８６に出力される。利用監視部１８６は、権利書データ１０６に基づいて、コンテンツの購入形態および利用形態が管理される。

【０２４５】次に、例えば、ユーザによって試聴モードが選択されると、既にセッション鍵データＫ$_{SES}$で復号されたコンテンツファイルＣＦのコンテンツデータＣと、スタックメモリ２００に記憶されたコンテンツ鍵データＫｃ、権利書データ１０６から得られた半開示パラメータデータ１９９およびユーザ電子透かし情報用データ１９６とが、相互認証を経た後に、図３８に示す復号・伸長モジュール管理部１８４を介して再生モジュール２７０に出力される。そして、再生モジュール２７０において、試聴モードに対応したコンテンツデータＣの再生が行われる。

【０２４６】次に、ユーザによる図３８に示す購入・利

106

用形態決定操作部１６５の操作によってコンテンツの購入・利用形態が決定され、当該決定に応じた操作信号Ｓ１６５が、課金処理部１８７に出力される。そして、課金処理部１８７において、決定された購入・利用形態に応じて利用制御状態データ１６６および利用履歴データ１０８が生成され、これがスタックメモリ２００および外部メモリ２０１にそれぞれ書き込まれる。次に、コンテンツ鍵データＫｃおよび利用制御状態データ１６６が、スタックメモリ２００から暗号化・復号部１７３に読み出され、暗号化・復号部１７３において記憶部１９２から読み出した記録用鍵データＫ$_{STR}$、メディア鍵データＫ$_{MED2}$および購入者鍵データＫ$_{PIN}$を用いて順に暗号化され、記録モジュール管理部８５５に出力される。そして、例えば、記録モジュール管理部８５５において、図３４（Ｃ）に示すキーファイルＫＦ$_1$が作成され、キーファイルＫＦ$_1$がメディアＳＡＭ管理部１９７を介してＲＡＭ型の記録媒体１３０$_5$のメディアＳＡＭ１３３に書き込まれる。また、セキュアコンテナ１０４ｙに格納されたコンテンツファイルＣＦは、記録モジュール管理部８５５によって、ＲＡＭ型の記録媒体１３０$_5$のＲＡＭ領域１３４に書き込まれる。また、利用制御状態データ１６６および利用履歴データ１０８は、所定のタイミングで、ＥＭＤサービスセンタ１０２に送信される。

【０２４７】以下、ＳＡＭ１０５$_1$～１０５$_4$の実現方法について説明する。ＳＡＭ１０５$_1$～１０５$_4$の機能をハードウェアとして実現する場合は、メモリを内蔵したＡＳＩＣ型のＣＰＵを用いて、そのメモリには、図２６に示す各機能を実現するためのセキュリティー機能モジュールやコンテンツの権利処理をおこなうプログラムモジュールおよび鍵データなどの機密度の高いデータが格納される。暗号ライブラリーモジュール（公開鍵暗号、共通鍵暗号、乱数発生器、ハッシュ関数）、コンテンツの使用制御用のプログラムモジュール、課金処理のプログラムモジュールなど、一連の権利処理用のプログラムモジュールは、例えば、ソフトウェアとして実装される。

【０２４８】例えば、図２６に示す暗号化・復号部１７１などのモジュールは、例えば、処理速度の問題でハードウエアとしてＡＳＩＣ型のＣＰＵ内のＩＰコアとして実装される。クロック速度やＣＰＵコード体系などの性能によっては、暗号化・復号部１７１をソフトウェアとして実装してもよい。また、図２６に示す記憶部１９２や、図２６に示す機能を実現するためのプログラムモジュールおよびデータを格納するメモリとしては、例えば、不揮発メモリー（フラッシュ－ＲＯＭ）が用いられ、作業用メモリとしてはＳＲＡＭなどの高速書き込み可能なメモリが用いられる。なお、その他にも、ＳＡＭ１０５$_1$～１０５$_4$に内蔵されるメモリとして、強誘電体メモリー（ＦｅＲＡＭ）を用いてもよい。また、ＳＡ

107

Ｍ１０５$_1$～１０５$_4$には、その他に、コンテンツの利用のための有効期限や契約期間などで日時の検証に使用する時計機能が内蔵されている。

【０２４９】上述したように、ＳＡＭ１０５$_1$～１０５$_4$は、プログラムモジュールや、データおよび処理内容を外部から遮蔽した耐タンパ性の構造を持っている。ＳＡＭ１０５$_1$～１０５$_4$を搭載した機器のホストＣＰＵのバス経由で、当該ＳＡＭのＩＣ内部のメモリに格納されている秘密性の高いプログラムおよびデータの内容や、ＳＡＭのシステムコンフイギュレーション（Ｓｙｓｔｅｍ　Ｃｏｎｆｉｇｕｒａｔｉｏｎ）関連のレジスタ群および暗号ライブラリーや時計のレジスタ群などの値が、読み出されたり、新規に書き込まれたりしないように、すなわち、搭載機器のホストＣＰＵが割り付けているアドレス空間内に存在しないように、当該ＳＡＭでは、ＣＰＵ側のメモリー空間を管理するＭＭＵ（Ｍｅｍｏｒｙ　Ｍａｇａｇｅｍｅｎｔ　Ｕｎｉｔ）を用いて、搭載機器側のホストＣＰＵからは見えないアドレス空間を設定する。また、ＳＡＭ１０５$_1$～１０５$_4$は、Ｘ線や熱などの外部からの物理的な攻撃にも耐え得る構造をもち、さらにデバッグ用ツール（ハードウエアＩＣＥ、ソフトウエアＩＣＥ）などを用いたリアルタイムデバッグ（リバースエンジニアリング）が行われても、その処理内容が分からないか、あるいは、デバッグ用ツールそのものがＩＣ製造後には使用できないような構造をしている。ＳＡＭ１０５$_1$～１０５$_4$自身は、ハードウエア的な構造においては、メモリを内蔵した通常のＡＳＩＣ型のＣＰＵであり、機能は当該ＣＰＵを動作させるソフトウェアに依存するが、暗号機能と耐タンパ性のハードウェア構造を有している点が、一般的なＡＳＩＣ型のＣＰＵと異なる。

【０２５０】ＳＡＭ１０５$_1$～１０５$_4$の機能を全てソフトウエアで実現する場合は、耐タンパ性を持ったモジュール内部で閉じてソフトウエア処理をおこなう場合と、通常のセットに搭載されているホストＣＰＵ上のソフトウエア処理で行い、当該処理のときにのみ解読することが不可能となる仕掛けをする場合とがある。前者は、暗号ライブラリモジュールがＩＰコアではなく、通常のソフトウェアモジュールとしてメモリに格納される場合と同じであり、ハードウェアとして実現する場合と同様に考えられる。一方、後者は、タンパーレジスタントソフトウェアと呼ばれるもので、ＩＣＥ（デバッガ）で実行状況を解読されても、そのタスクの実行順序がバラバラであったり（この場合には、区切ったタスク単体でプログラムとしての意味があるように、すなわち前後のラインに影響がでないようにタスク切りを行う）、タスクそのものが暗号化されており、一種のセキュア処理を目的としたタスクスケジューラ（ＭｉｎｉＯＳ）と同様に実現できる。当該タスクスケジューラは、ターゲットプログラムに埋め込まれている。

108

【０２５１】次に、図２５に示す復号・伸長モジュール１６３について説明する。図２５に示すように、復号・伸長モジュール１６３は、相互認証部２２０、復号部２２１、復号部２２２、伸長部２２３、電子透かし情報処理部２２４および半開示処理部２２５を有する。相互認証部２２０は、復号・伸長モジュール１６３がＳＡＭ１０５$_1$からデータを入力する際に、図３２に示す相互認証部１７０との間で相互認証を行ってセッション鍵データＫ$_{SES}$を生成する。

【０２５２】復号部２２１は、ＳＡＭ１０５$_1$から入力したコンテンツ鍵データＫｃ、半開示パラメータデータ１９９、ユーザ電子透かし情報用データ１９６およびコンテンツデータＣを、セッション鍵データＫ$_{SES}$を用いて復号する。そして、復号部２２１は、復号したコンテンツ鍵データＫｃおよびコンテンツデータＣを復号部２２２に出力し、復号したユーザ電子透かし情報用データ１９６を電子透かし情報処理部２２４に出力し、半開示パラメータデータ１９９を半開示処理部２２５に出力する。

【０２５３】復号部２２２は、半開示処理部２２５からの制御に基づいて、コンテンツ鍵データＫｃを用いて、コンテンツデータＣを半開示状態で復号し、復号したコンテンツデータＣを伸長部２２３に出力する。

【０２５４】伸長部２２３は、復号されたコンテンツデータＣを伸長して、電子透かし情報処理部２２４に出力する。伸長部２２３は、例えば、図５（Ａ）に示すコンテンツファイルＣＦに格納されたＡ／Ｖ伸長用ソフトウェアを用いて伸長処理を行い、例えば、ＡＴＲＡＣ３方式で伸長処理を行う。

【０２５５】電子透かし情報処理部２２４は、復号されたユーザ電子透かし情報用データ１９６に応じたユーザ電子透かし情報を、復号されたコンテンツデータＣに埋め込み、新たなコンテンツデータＣを生成する。電子透かし情報処理部２２４は、当該新たなコンテンツデータＣを再生モジュール１６９に出力する。このように、ユーザ電子透かし情報は、コンテンツデータＣを再生するときに、復号・伸長モジュール１６３において埋め込まれる。なお、本発明では、コンテンツデータＣにユーザ電子透かし情報用データ１９６を埋め込まないようにしてもよい。

【０２５６】半開示処理部２２５は、半開示パラメータデータ１９９に基づいて、例えば、コンテンツデータＣのうち復号を行わないブロックと、復号を行うブロックとを復号部２２２に指示する。また、半開示処理部２２５は、その他に、半開示パラメータデータ１９９に基づいて、試聴時の再生機能を限定したり、試聴可能な期間を限定するなどの制御を行う。

【０２５７】再生モジュール１６９は、復号および伸長されたコンテンツデータＣに応じた再生を行う。

【０２５８】次に、コンテンツプロバイダ１０１、ＥＭ

Dサービスセンタ１０２およびユーザホームネットワーク１０３の間で、秘密鍵データを用いて生成した署名データを付したデータおよび公開鍵証明書データを送受信する際のデータフォーマットについて説明する。図４２（A）は、コンテンツプロバイダ１０１からＳＡＭ１０５$_1$にデータＤａｔａをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、コンテンツプロバイダ１０１からＳＡＭ１０５$_1$に、コンテンツプロバイダ１０１とＳＡＭ１０５$_1$との間の相互認証によって得たセッション鍵データK_{SES}で暗号化したモジュールＭｏｄ$_{50}$が送信される。モジュールＭｏｄ$_{50}$には、モジュールＭｏｄ$_{51}$およびその秘密鍵データ$K_{CP,S}$による署名データSIG_{CP}が格納されている。モジュールＭｏｄ$_{51}$には、コンテンツプロバイダ１０１の秘密鍵データ$K_{CP,P}$を格納した公開鍵証明書データCER_{CP}と、公開鍵証明書データCER_{CP}に対しての秘密鍵データ$K_{ESC,S}$による署名データSIG_{ESC}と、送信するデータＤａｔａとが格納されている。このように、公開鍵証明書データCER_{CP}を格納したモジュールＭｏｄ$_{50}$を、コンテンツプロバイダ１０１からＳＡＭ１０５$_1$に送信することで、ＳＡＭ１０５$_1$において署名データSIG_{CP}の検証を行なう際に、ＥＭＤサービスセンタ１０２からＳＡＭ１０５$_1$に公開鍵証明書データCER_{CP}を送信する必要がなくなる。

【０２５９】図４２（Ｂ），（Ｃ）は、コンテンツプロバイダ１０１からＳＡＭ１０５$_1$にデータＤａｔａをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、コンテンツプロバイダ１０１からＳＡＭ１０５$_1$に、コンテンツプロバイダ１０１とＳＡＭ１０５$_1$との間の相互認証によって得たセッション鍵データK_{SES}で暗号化した図４２（Ｂ）に示すモジュールＭｏｄ$_{52}$が送信される。モジュールＭｏｄ$_{52}$には、送信するデータＤａｔａと、その秘密鍵データ$K_{CP,S}$による署名データSIG_{CP}とが格納されている。また、ＥＭＤサービスセンタ１０２からＳＡＭ１０５$_1$には、ＥＭＤサービスセンタ１０２とＳＡＭ１０５$_1$との間の相互認証によって得たセッション鍵データK_{SES}で暗号化した図４２（Ｃ）に示すモジュールＭｏｄ$_{53}$が送信される。モジュールＭｏｄ$_{53}$には、コンテンツプロバイダ１０１の公開鍵証明書データCER_{CP}と、その秘密鍵データ$K_{ESC,S}$による署名データSIG_{ESC}とが格納されている。

【０２６０】図４２（Ｄ）は、ＳＡＭ１０５$_1$からコンテンツプロバイダ１０１にデータＤａｔａをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、ＳＡＭ１０５$_1$からコンテンツプロバイダ１０１に、コンテンツプロバイダ１０１とＳＡＭ１０５$_1$との間の相互認証によって得たセッション鍵データK_{SES}で暗号化したモジュールＭｏｄ$_{54}$が送信される。モジュールＭｏｄ$_{54}$には、モジュールＭｏｄ$_{55}$およびその秘密鍵データ$K_{SAM1,S}$による署名データSIG_{SAM1}が格納されている。モジュールＭｏｄ$_{55}$には、ＳＡＭ１０５$_1$の秘密鍵データ$K_{SAM1,P}$を格納した公開鍵証明書データCER_{SAM1}と、公開鍵証明書データCER_{SAM1}に対しての秘密鍵データ$K_{ESC,S}$による署名データSIG_{ESC}と、送信するデータＤａｔａとが格納されている。このように、公開鍵証明書データCER_{SAM1}を格納したモジュールＭｏｄ$_{55}$を、ＳＡＭ１０５$_1$からコンテンツプロバイダ１０１に送信することで、コンテンツプロバイダ１０１において署名データSIG_{SAM1}の検証を行なう際に、ＥＭＤサービスセンタ１０２からコンテンツプロバイダ１０１に公開鍵証明書データCER_{SAM1}を送信する必要がなくなる。

【０２６１】図４２（Ｅ），（Ｆ）は、ＳＡＭ１０５$_1$からコンテンツプロバイダ１０１にデータＤａｔａをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、ＳＡＭ１０５$_1$からコンテンツプロバイダ１０１に、コンテンツプロバイダ１０１とＳＡＭ１０５$_1$との間の相互認証によって得たセッション鍵データK_{SES}で暗号化した図４２（Ｅ）に示すモジュールＭｏｄ$_{56}$が送信される。モジュールＭｏｄ$_{56}$には、送信するデータＤａｔａと、その秘密鍵データ$K_{SAM1,S}$による署名データSIG_{SAM1}とが格納されている。また、ＥＭＤサービスセンタ１０２からコンテンツプロバイダ１０１には、ＥＭＤサービスセンタ１０２とコンテンツプロバイダ１０１との間の相互認証によって得たセッション鍵データK_{SES}で暗号化した図４２（Ｆ）に示すモジュールＭｏｄ$_{57}$が送信される。モジュールＭｏｄ$_{57}$には、ＳＡＭ１０５$_1$の公開鍵証明書データCER_{SAM1}と、その秘密鍵データ$K_{ESC,S}$による署名データSIG_{ESC}とが格納されている。

【０２６２】図４３（Ｇ）は、コンテンツプロバイダ１０１からＥＭＤサービスセンタ１０２にデータＤａｔａをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、コンテンツプロバイダ１０１からＥＭＤサービスセンタ１０２に、コンテンツプロバイダ１０１とＥＭＤサービスセンタ１０２との間の相互認証によって得たセッション鍵データK_{SES}で暗号化したモジュールＭｏｄ$_{58}$が送信される。モジュールＭｏｄ$_{58}$には、モジュールＭｏｄ$_{59}$およびその秘密鍵データ$K_{CP,S}$による署名データSIG_{CP}が格納されている。モジュールＭｏｄ$_{59}$には、コンテンツプロバイダ１０１の秘密鍵データ$K_{CP,P}$を格納した公開鍵証明書データCER_{CP}と、公開鍵証明書データCER_{CP}に対しての秘密鍵データ$K_{ESC,S}$による署名データSIG_{ESC}と、送信す

るデータＤａｔａとが格納されている。

【０２６３】図４３（Ｈ）は、コンテンツプロバイダ１０１からＥＭＤサービスセンタ１０２にデータＤａｔａをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、コンテンツプロバイダ１０１からＥＭＤサービスセンタ１０２に、コンテンツプロバイダ１０１とＥＭＤサービスセンタ１０２との間の相互認証によって得たセッション鍵データK_{SES}で暗号化した図４３（Ｈ）に示すモジュールMod_{60}が送信される。モジュールMod_{60}には、送信するデータＤａｔａと、その秘密鍵データ$K_{CP,S}$による署名データSIG_{CP}とが格納されている。このとき、ＥＭＤサービスセンタ１０２にはコンテンツプロバイダ１０１の公開鍵証明書データCER_{CP}は既に登録されている。

【０２６４】図４３（Ｉ）は、$SAM105_1$からＥＭＤサービスセンタ１０２にデータＤａｔａをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、$SAM105_1$からＥＭＤサービスセンタ１０２に、ＥＭＤサービスセンタ１０２と$SAM105_1$との間の相互認証によって得たセッション鍵データK_{SES}で暗号化したモジュールMod_{61}が送信される。モジュールMod_{61}には、モジュールMod_{62}およびその秘密鍵データ$K_{SAM1,S}$による署名データSIG_{SAM1}が格納されている。モジュールMod_{62}には、$SAM105_1$の秘密鍵データ$K_{SAM1,P}$を格納した公開鍵証明書データCER_{SAM1}と、公開鍵証明書データCER_{SAM1}に対しての秘密鍵データ$K_{ESC,S}$による署名データSIG_{ESC}と、送信するデータＤａｔａとが格納されている。

【０２６５】図４３（Ｊ）は、$SAM105_1$からＥＭＤサービスセンタ１０２にデータＤａｔａをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。この場合には、$SAM105_1$からＥＭＤサービスセンタ１０２に、ＥＭＤサービスセンタ１０２と$SAM105_1$との間の相互認証によって得たセッション鍵データK_{SES}で暗号化した図４３（Ｊ）に示すモジュールMod_{63}が送信される。モジュールMod_{63}には、送信するデータＤａｔａと、その秘密鍵データ$K_{SAM1,S}$による署名データSIG_{SAM1}とが格納されている。このとき、ＥＭＤサービスセンタ１０２には$SAM105_1$の公開鍵証明書データCER_{SAM1}は既に登録されている。

【０２６６】以下、$SAM105_1$～105_4の出荷時におけるＥＭＤサービスセンタ１０２への登録処理について説明する。なお、$SAM105_1$～105_4の登録処理は同じであるため、以下、$SAM105_1$の登録処理について述べる。$SAM105_1$の出荷時には、図２４に示すＥＭＤサービスセンタ１０２の鍵サーバ１４１

によって、ＳＡＭ管理部１４９を介して、図２６などに示す記憶部１９２に以下に示す鍵データが初期登録される。また、$SAM105_1$には、例えば、出荷時に、記憶部１９２などに、$SAM105_1$がＥＭＤサービスセンタ１０２に初回にアクセスする際に用いられるプログラムなどが記憶される。すなわち、記憶部１９２には、例えば、図３０において左側に「＊」が付されている$SAM105_1$の識別子ＳＡＭ＿ＩＤ、記録用鍵データK_{STR}、ルート認証局２の公開鍵データK_{R-CA}、ＥＭＤサービスセンタ１０２の公開鍵データ$K_{ESC,P}$、$SAM105_1$の秘密鍵データ$K_{SAM1,S}$、公開鍵証明書データCER_{SAM1}およびその署名データ$SIG_{22,ESC}$、復号・伸長モジュール１６３およびメディアＳＡＭとの間の認証用鍵データを生成するための元鍵データが初期登録で記憶される。なお、公開鍵証明書データCER_{SAM1}は、$SAM105_1$を出荷後に登録する際にＥＭＤサービスセンタ１０２から$SAM105_1$に送信してもよい。

【０２６７】また、記憶部１９２には、$SAM105_1$の出荷時に、図５に示すコンテンツファイルＣＦおよびキーファイルＫＦを読み込み形式を示すファイルリーダが、ＥＭＤサービスセンタ１０２によって書き込まれる。$SAM105_1$では、コンテンツファイルＣＦおよびキーファイルＫＦに格納されたデータを利用する際に、記憶部１９２に記憶されたファイルリーダが用いられる。

【０２６８】ここで、ルート認証局２の公開鍵データK_{R-CA}は、インターネットの電子商取引などでは一般的に使用されているＲＳＡを使用し、データ長は例えば１０２４ビットである。公開鍵データK_{R-CA}は、図１に示すルート認証局２によって発行される。また、ＥＭＤサービスセンタ１０２の公開鍵データ$K_{ESC,P}$は、短いデータ長でＲＳＡと同等あるいはそれ以上の強度を持つ楕円曲線暗号を利用して生成され、データ長は例えば１６０ビットである。但し、暗号化の強度を考慮すると、公開鍵データ$K_{ESC,P}$は１９２ビット以上であることが望ましい。また、ＥＭＤサービスセンタ１０２は、ルート認証局９２に公開鍵データ$K_{ESC,P}$を登録する。また、ルート認証局９２は、公開鍵データ$K_{ESC,P}$の公開鍵証明書データCER_{ESC}を作成する。公開鍵データ$K_{ESC,P}$を格納した公開鍵証明書データCER_{ESC}は、好ましく、$SAM105_1$の出荷時に記憶部１９２に記憶される。この場合に、公開鍵証明書データCER_{ESC}は、ルート認証局９２の秘密鍵データ$K_{ROOT,S}$で署名されている。

【０２６９】ＥＭＤサービスセンタ１０２は、乱数を発生して$SAM105_1$の秘密鍵データ$K_{SAM1,S}$、を生成し、これとペアとなる公開鍵データ$K_{SAM1,P}$を生成する。また、ＥＭＤサービスセンタ１０２は、ルート認証局９２の認証をもらって、公開鍵

データ$K_{SAM1,P}$の公開鍵証明書データCER_{SAM1}を発行し、これに自らの秘密鍵データ$K_{ESC,S}$を用いて署名データを添付する。すなわち、ＥＭＤサービスセンタ１０２は、セカンドＣＡ（認証局）として機能を果たす。

【０２７０】また、ＳＡＭ１０５$_1$には、図２４に示すＥＭＤサービスセンタ１０２のＳＡＭ管理部１４９により、ＥＭＤサービスセンタ１０２の管理下にある一意（ユニーク）な識別子ＳＡＭ＿ＩＤが割り当てられ、これがＳＡＭ１０５$_1$の記憶部１９２に格納されると共に、図２４に示すＳＡＭデータベース１４９ａにも格納され、ＥＭＤサービスセンタ１０２によって管理される。

【０２７１】また、ＳＡＭ１０５$_1$は、出荷後、例えば、ユーザによってＥＭＤサービスセンタ１０２と接続され、登録手続を行うと共に、ＥＭＤサービスセンタ１０２から記憶部１９２に配信用鍵データＫＤ$_1$～ＫＤ$_3$が転送される。すなわち、ＳＡＭ１０５$_1$を利用するユーザは、コンテンツをダウンロードする前にＥＭＤサービスセンタ１０２に登録手続が必要である。この登録手続は、例えば、ＳＡＭ１０５$_1$を搭載している機器（当該例では、ネットワーク機器１６０$_1$）を購入したときに添付された登録用紙などを用いて、ユーザ本人が自己を特定する情報を記載して例えば郵便などのオフラインで行なわれる。ＳＡＭ１０５$_1$は、上述した登録手続を経た後でないと使用できない。

【０２７２】ＥＭＤサービスセンタ１０２は、ＳＡＭ１０５$_1$のユーザによる登録手続に応じて、ユーザに固有の識別子ＵＳＥＲ＿ＩＤを発行し、例えば、図２４に示すＳＡＭデータベース１４９ａにおいて、ＳＡＭ＿ＩＤとＵＳＥＲ＿ＩＤとの対応関係を管理し、課金時に利用する。また、ＥＭＤサービスセンタ１０２は、ＳＡＭ１０５$_1$のユーザに対して情報参照用識別子ＴＤと、初回に使用されるパスワードを割り当て、これをユーザに通知する。ユーザは、情報参照用識別子ＩＤとパスワードとを用いて、ＥＭＤサービスセンタ１０２に、例えば現在までのコンテンツデータの利用状況（利用履歴）などを情報の問い合わせを行なうことができる。また、ＥＭＤサービスセンタ１０２は、ユーザの登録時に、クレジットカード会社などに身分の確認を行なったり、オフラインで本人の確認を行なう。

【０２７３】次に、図３０に示すように、ＳＡＭ１０５$_1$内の記憶部１９２にＳＡＭ登録リストを格納する手順について説明する。図１に示すＳＡＭ１０５$_1$は、例えば、バス１９１としてＩＥＥＥ１３９４シリアルバスを用いた場合に、バス１９１に接続された機器の電源を立ち上げたり、新しい機器をバス１９１に接続したときに生成されるトポロジーマップを利用して、自分の系に存在するＳＡＭ１０５$_2$～ＳＡＭ１０５$_4$のＳＡＭ登録リストを得る。なお、ＩＥＥＥ１３９４シリアルバスであるバス１９１に応じて生成されたトポロジーマップは、例えば、図４４に示すように、バス１９１にＳＡＭ１０５$_1$～１０５$_4$に加えてＡＶ機器１６０$_5$，１６０$_6$のＳＣＭＳ処理回路１０５$_5$，１０５$_6$が接続されている場合に、ＳＡＭ１０５$_1$～１０５$_4$およびＳＣＭＳ処理回路１０５，１０５$_6$を対象として生成される。従って、ＳＡＭ１０５$_1$は、当該トポロジーマップから、ＳＡＭ１０５$_1$～１０５$_4$についての情報を抽出して図４５に示すＳＡＭ登録リストを生成する。

【０２７４】そして、ＳＡＭ１０５$_1$は、図４５に示すＳＡＭ登録リストを、ＥＭＤサービスセンタ１０２に登録して署名を得る。これらの処理は、バス１９１のセッションを利用してＳＡＭ１０５$_1$が自動的に行い、ＥＭＤサービスセンタ１０２にＳＡＭ登録リストの登録命令を発行する。ＥＭＤサービスセンタ１０２は、ＳＡＭ１０５$_1$から図４５に示すＳＡＭ登録リストを受けると、有効期限を確認する。そして、ＥＭＤサービスセンタ１０２は、登録時にＳＡＭ１０５$_1$より指定された決済機能の有無を参照して対応する部分の設定を行う。また、ＥＭＤサービスセンタ１０２は、リボケーションリストをチェックしてＳＡＭ登録リスト内のリボケーションフラグを設定する。リボケーションリストは、例えば、不正使用などを理由にＥＭＤサービスセンタ１０２によって使用が禁止されている（無効な）ＳＡＭのリストである。また、ＥＭＤサービスセンタ１０２は、決済時にはＳＡＭ１０５$_1$に対応するＳＡＭ登録リストを取り出し、その中に記述されたＳＡＭがリボケーションリストに含まれているかを確認する。また、ＥＭＤサービスセンタ１０２は、ＳＡＭ登録リストに署名を添付する。これにより、図４６に示すＳＡＭ登録リストが作成される。なお、ＳＡＭリボケーションリストは、同一系の（同一のバス１９１に接続されている）ＳＡＭのみを対象として生成され、各ＳＡＭに対応するリボケーションフラグによって、当該ＳＡＭの有効および無効を示している。

【０２７５】以下、図１に示すコンテンツプロバイダ１０１の全体動作について説明する。図４７は、コンテンツプロバイダ１０１の全体動作のフローチャートである。

ステップＳ１：ＥＭＤサービスセンタ１０２は、コンテンツプロバイダ１０１が所定の登録処理を経た後に、コンテンツプロバイダ１０１の公開鍵データ$K_{CP,P}$の公開鍵証明書CER_{CP}をコンテンツプロバイダ１０１に送信する。また、ＥＭＤサービスセンタ１０２は、ＳＡＭ１０５$_1$～１０５$_4$が所定の登録処理を経た後に、ＳＡＭ１０５$_1$～１０５$_4$の公開鍵データ$K_{SAM1,P}$～$K_{SAM4,P}$の公開鍵証明書CER_{CP1}～CER_{CP4}をＳＡＭ１０５$_1$～１０５$_4$に送信する。また、ＥＭＤサービスセンタ１０２は、相互認証を行った後に、各々有効期限が１カ月の３カ月分の配

115

信用鍵データＫＤ１～ＫＤ３をユーザホームネットワーク１０３のＳＡＭ１０５１～１０５４に送信する。このように、ＥＭＤシステム１００では、配信用鍵データＫＤ１～ＫＤ３を予めＳＡＭ１０５１～１０５４に配給しているため、ＳＡＭ１０５１～１０５４とＥＭＤサービスセンタ１０２との間がオフラインの状態でも、ＳＡＭ１０５１～１０５４においてコンテンツプロバイダ１０１から配給されたセキュアコンテナ１０４を復号して購入・利用できる。この場合に、当該購入・利用の履歴は利用履歴データ１０８に記述され、利用履歴データ１０８は、ＳＡＭ１０５１～１０５４とＥＭＤサービスセンタ１０２とが接続されたときに、ＥＭＤサービスセンタ１０２に自動的に送信されるため、ＥＭＤサービスセンタ１０２における決済処理を確実に行うことができる。なお、ＥＭＤサービスセンタ１０２が、所定の期間内に、利用履歴データ１０８を回収できないＳＡＭについては、リボケーションリストで無効の対象とする。なお、利用制御状態データ１６６は、原則として、リアルタイムで、ＳＡＭ１０５１～１０５４からＥＭＤサービスセンタ１０２に送信される。

【０２７６】ステップＳ２：コンテンツプロバイダ１０１は、相互認証を行った後に、図１８に示す登録用モジュールＭｏｄ２を、ＥＭＤサービスセンタ１０２に送信する。そして、ＥＭＤサービスセンタ１０２は、所定の署名検証を行った後に、権利書データ１０６およびコンテンツ鍵データＫｃを登録して権威化する。また、ＥＭＤサービスセンタ１０２は、登録用モジュールＭｏｄ２に応じた６カ月分のキーファイルＫＦを作成し、これをコンテンツプロバイダ１０１に送信する。

【０２７７】ステップＳ３：コンテンツプロバイダ１０１は、図５（Ａ），（Ｂ）に示すコンテンツファイルＣＦおよびその署名データＳＩＧ６，ＣＰと、キーファイルＫＦおよびその署名データＳＩＧ７，ＣＰとを作成し、これらと図５（Ｃ）に示す公開鍵証明書データＣＥＲＣＰおよびその署名データＳＩＧ１，ＥＳＣとを格納したセキュアコンテナ１０４を、オンラインおよび／またはオフラインで、ユーザホームネットワーク１０３のＳＡＭ１０５１～１０５４に配給する。オンラインの場合には、コンテンツプロバイダ用配送プロトコルを用いられ、当該プロトコルに依存しない形式で（すなわち、複数階層からなる通信プロトコルの所定の層を用いて伝送されるデータとして）、セキュアコンテナ１０４がコンテンツプロバイダ１０１からユーザホームネットワーク１０３に配送される。また、オフラインの場合には、ＲＯＭ型あるいはＲＡＭ型の記録媒体に記録された状態で、セキュアコンテナ１０４が、コンテンツプロバイダ１０１からユーザホームネットワーク１０３に配送される。

【０２７８】ステップＳ４：ユーザホームネットワーク１０３のＳＡＭ１０５１～ＳＡＭ１０５４は、コンテンツプロバイダ１０１から配給を受けたセキュアコンテナ１０４内の署名データＳＩＧ６，ＣＰ，ＳＩＧ７，ＣＰ，ＳＩＧＫ１，ＥＳＣを検証して、コンテンツファイルＣＦおよびキーファイルＫＦの作成者および送信者の正当性を確認した後に、対応する期間の配信用鍵データＫＤ１～ＫＤ６を用いてキーファイルＫＦを復号する。

116

【０２７９】ステップＳ５：ＳＡＭ１０５１～ＳＡＭ１０５４において、ユーザによる図２５に示す購入・利用形態決定操作部１６５の操作に応じた操作信号Ｓ１６５に基づいて、購入・利用形態を決定する。このとき、図３１に示す利用監視部１８６において、セキュアコンテナ１０４に格納された権利書データ１０６に基づいて、ユーザによるコンテンツファイルＣＦの購入・利用形態が管理される。

【０２８０】ステップＳ６：ＳＡＭ１０５１～ＳＡＭ１０５４の図３１に示す課金処理部１８７において、操作信号Ｓ１６５に基づいて、ユーザによる購入・利用形態の決定の操作を記述した利用履歴データ１０８および利用制御状態データ１６６が生成し、これらをＥＭＤサービスセンタ１０２に送信する。

【０２８１】ステップＳ７：ＥＭＤサービスセンタ１０２は、図２４に示す決算処理部１４２において、利用履歴データ１０８に基づいて決済処理を行い、決済請求権データ１５２および決済レポートデータ１０７を作成する。ＥＭＤサービスセンタ１０２は、決済請求権データ１５２およびその署名データＳＩＧ９９を、図１に示すペイメントゲートウェイ９０を介して、決済機関９１に送信する。また、ＥＭＤサービスセンタ１０２は、決済レポートデータ１０７をコンテンツプロバイダ１０１に送信する。

【０２８２】ステップＳ８：　決済機関９１において、署名データＳＩＧ９９の検証を行った後に、決済請求権データ１５２に基づいて、ユーザが支払った金額が、コンテンツプロバイダ１０１の所有者に分配される。

【０２８３】以上説明したように、ＥＭＤシステム１００では、図５に示すフォーマットのセキュアコンテナ１０４をコンテンツプロバイダ１０１からユーザホームネットワーク１０３に配給し、セキュアコンテナ１０４内のキーファイルＫＦについての処理をＳＡＭ１０５１～１０５４内で行う。また、キーファイルＫＦに格納されたコンテンツ鍵データＫｃおよび権利書データ１０６は、配信鍵データＫＤ１～ＫＤ３を用いて暗号化されており、配信鍵データＫＤ１～ＫＤ３を保持しているＳＡＭ１０５１～１０５４内でのみ復号される。そして、ＳＡＭ１０５１～１０５４では、耐タンパ性を有するモジュールであり、権利書データ１０６に記述されたコンテンツデータＣの取り扱い内容に基づいて、コンテンツデータＣの購入形態および利用形態が決定される。従って、ＥＭＤシステム１００によれば、ユーザホームネッ

トワーク１０３におけるコンテンツデータＣの購入および利用を、コンテンツプロバイダ１０１の関係者が作成した権利書データ１０６の内容に基づいて確実に行わせることができる。

【０２８４】また、ＥＭＤシステム１００では、コンテンツプロバイダ１０１からユーザホームネットワーク１０３へのコンテンツデータＣの配給を、オンラインおよびオフラインの何れの場合でもセキュアコンテナ１０４を用いて行うことで、ＳＡＭ105_1～105_4におけるコンテンツデータＣの権利処理を双方の場合において共通化できる。

【０２８５】また、ＥＭＤシステム１００では、ユーザホームネットワーク１０３内のネットワーク機器160_1およびＡＶ機器160_2～160_4においてコンテンツデータＣを購入、利用、記録および転送する際に、常に権利書データ１０６に基づいて処理を行うことで、共通の権利処理ルールを採用できる。

【０２８６】図４８は、第１実施形態で採用されるセキュアコンテナの配送プロトコルの一例を説明するための図である。図４８に示すように、マルチプロセッサシステム１００では、コンテンツプロバイダ１０１からユーザホームネットワーク１０３にセキュアコンテナ１０４を配送するプロトコルとして例えばＴＣＰ／ＩＰおよびＸＭＬ／ＳＭＩＬが用いられる。また、ユーザホームネットワーク１０３のＳＡＭ相互間でセキュアコンテナを転送するプロトコル、並びにユーザホームネットワーク１０３と１０３ａとの間でセキュアコンテナを転送するプロトコルとして例えば１３９４シリアルバス・インタフェース上に構築されたＸＭＬ／ＳＭＩＬが用いられる。また、この場合に、ＲＯＭ型やＲＡＭ型の記録媒体にセキュアコンテナを記録してＳＡＭ相互間で配送してもよい。

【０２８７】第１実施形態の第１変形例

上述した実施形態では、図５（Ｂ）に示すように、ＥＭＤサービスセンタ１０２において配信用鍵データＫＤを用いてキーファイルＫＦを暗号化し、ＳＡＭ105_1～105_4において配信用鍵データＫＤを用いてキーファイルＫＦを復号する場合を例示したが、図１に示すように、コンテンツプロバイダ１０１からＳＡＭ105_1～105_4にセキュアコンテナ１０４を直接供給する場合には、配信用鍵データＫＤを用いたキーファイルＫＦの暗号化は必ずしも行なわなくてもよい。このように、配信用鍵データＫＤを用いてキーファイルＫＦを暗号化することは、後述する第２実施形態のように、コンテンツプロバイダからユーザホームネットワークにサービスプロバイダを介してコンテンツデータを供給する場合に、配信用鍵データＫＤをコンテンツプロバイダおよびユーザホームネットワークにのみ保持させることで、サービスプロバイダによる不正行為を抑制する際に大きな効果を発揮する。但し、上述した第１実施形態の場合でも、配信用鍵データＫＤを用いてキーファイルＫＦを暗号化することは、コンテンツデータの不正利用の抑制力を高める点で効果がある。

【０２８８】また、上述した実施形態では、図５（Ｂ）に示すキーファイルＫＦ内の権利書データ１０６内に標準小売価格データＳＲＰを格納する場合を例示したが、セキュアコンテナ１０４内のキーファイルＫＦの外に、標準小売価格データＳＲＰ（プライスタグデータ）を格納してもよい。この場合には、標準小売価格データＳＲＰに対して秘密鍵データ$Ｋ_{ｃｐ}$を用いて作成した署名データを添付する。

【０２８９】第１実施形態の第２変形例

上述した第１実施形態では、図１に示すように、ＥＭＤサービスセンタ１０２が、自らが生成した決済請求権データ１５２を用いて、ペイメントゲートウェイ９０を介して決済機関９１で決済処理を行なう場合を例示したが、例えば、図４９に示すように、ＥＭＤサービスセンタ１０２からコンテンツプロバイダ１０１に決済請求権データ１５２を送信し、コンテンツプロバイダ１０１自らが、決済請求権データ１５２を用いて、ペイメントゲートウェイ９０を介して決済機関９１に対して決済処理を行なってもよい。

【０２９０】第１実施形態の第３変形例

上述した第１実施形態では、単数のコンテンツプロバイダ１０１からユーザホームネットワーク１０３のＳＡＭ105_1～105_4に、セキュアコンテナ１０４を供給する場合を例示したが、２以上のコンテンツプロバイダ１０１ａ，１０１ｂからＳＡＭ105_1～105_4にそれぞれセキュアコンテナ１０４ａ，１０４ｂを供給するようにしてもよい。図５０は、コンテンツプロバイダ１０１ａ，１０１ｂを用いる場合の第１実施形態の第３変形例に係わるＥＭＤシステムの構成図である。この場合には、ＥＭＤサービスセンタ１０２は、コンテンツプロバイダ１０１ａおよび１０１ｂに、それぞれの６カ月分の配信用鍵データ$ＫＤａ_1$～$ＫＤａ_6$および$ＫＤｂ_1$～$ＫＤｂ_6$を用いて暗号化したキーファイル$ＫＦａ_1$～$ＫＦａ_6$および$ＫＦｂ_1$～$ＫＦｂ_6$を配信する。また、ＥＭＤサービスセンタ１０２は、ＳＡＭ105_1～105_4に、３カ月分の配信用鍵データ$ＫＤａ_1$～$ＫＤａ_3$および$ＫＤｂ_1$～$ＫＤｂ_3$を配信する。

【０２９１】そして、コンテンツプロバイダ１０１ａは、独自のコンテンツ鍵データ$Ｋｃａ$を用いて暗号化したコンテンツファイルＣＦａと、ＥＭＤサービスセンタ１０２から受信した対応する期間のキーファイル$ＫＦａ_1$～$ＫＦａ_6$とを格納したセキュアコンテナ１０４ａをＳＡＭ105_1～105_4にオンラインおよび／またはオフランで供給する。このとき、キーファイルの識別子として、ＥＭＤサービスセンタ１０２が配付するグローバルユニークな識別子コンテンツＩＤが用いられ、ＥＭＤサービスセンタ１０２によって、コンテンツデータが

一元的に管理される。また、コンテンツプロバイダ１０１ｂは、独自のコンテンツ鍵データＫｃｂを用いて暗号化したコンテンツファイルＣＦｂと、ＥＭＤサービスセンタ１０２から受信した対応する期間のキーファイルＫＦｂ$_1$～ＫＦｂ$_6$とを格納したセキュアコンテナ１０４ｂをＳＡＭ１０５$_1$～１０５$_4$にオンラインおよび／またはオフラインで供給する。

【０２９２】ＳＡＭ１０５$_1$～１０５$_4$は、セキュアコンテナ１０４ａについては、対応する期間の配信用鍵データＫＤａ$_1$～ＫＤａ$_3$を用いて復号を行い、所定の署名検証処理などを経てコンテンツの購入形態を決定し、当該決定された購入形態および利用形態などに応じて生成した利用履歴データ１０８ａおよび利用制御状態データ１６６ａをＥＭＤサービスセンタ１０２に送信する。また、ＳＡＭ１０５$_1$～１０５$_4$は、セキュアコンテナ１０４ｂについては、対応する期間の配信用鍵データＫＤｂ$_1$～ＫＤｂ$_3$を用いて復号を行い、所定の署名検証処理などを経てコンテンツの購入形態を決定し、当該決定された購入形態および利用形態などに応じて生成した利用履歴データ１０８ｂおよび利用制御状態データ１６６ｂをＥＭＤサービスセンタ１０２に送信する。

【０２９３】ＥＭＤサービスセンタ１０２では、利用履歴データ１０８ａに基づいて、コンテンツプロバイダ１０１ａについての決済請求権データ１５２ａを作成し、これを用いて決済機関９１に対して決済処理を行なう。また、ＥＭＤサービスセンタ１０２では、利用履歴データ１０８ｂに基づいて、コンテンツプロバイダ１０１ｂについての決済請求権データ１５２ｂを作成し、これを用いて決済機関９１に対して決済処理を行なう。

【０２９４】また、ＥＭＤサービスセンタ１０２は、権利書データ１０６ａ，１０６ｂを登録して権威化を行なう。このとき、ＥＭＤサービスセンタ１０２は、権利書データ１０６ａ，１０６ｂに対応するキーファイルＫＦａ，ＫＦｂに対して、グローバルユニークな識別子コンテンツＩＤを配付する。また、ＥＭＤサービスセンタ１０２は、コンテンツプロバイダ１０１ａ，１０１ｂの公開鍵証明書データＣＥＲ$_{cpa}$，ＣＥＲ$_{cpb}$を発行し、これに自らの署名データＳＩＧ$_{1b,esc}$，ＳＩＧ$_{1a,esc}$を付してその正当性を認証する。

【０２９５】第１実施形態の第４変形例

上述した実施形態では、コンテンツファイルＣＦおよびキーファイルＫＦをディレクトリ構造でセキュアコンテナ１０４内に格納してコンテンツプロバイダ１０１からＳＡＭ１０５$_1$～１０５$_4$に送信する場合を例示したが、コンテンツファイルＣＦおよびキーファイルＫＦを、別々にＳＡＭ１０５$_1$～１０５$_4$に送信してもよい。これには、例えば、以下に示す第１の手法と第２の手法とがある。第１の手法では、図５１に示すように、コンテンツプロバイダ１０１からＳＡＭ１０５$_1$～１０５$_4$に、通信プロトコルに依存しない形式で、コンテンツファイルＣＦおよびキーファイルＫＦを別々に送信する。また、第２の手法では、図５２に示すように、コンテンツプロバイダ１０１からＳＡＭ１０５$_1$～１０５$_4$にコンテンツファイルＣＦを通信プロトコルに依存しない形式で送信すると共に、ＥＭＤサービスセンタ１０２からＳＡＭ１０５$_1$～１０５$_4$にキーファイルＫＦを送信する。当該キーファイルＫＦの送信は、例えば、ＳＡＭ１０５$_1$～１０５$_4$のユーザが、コンテンツデータＣの購入形態を決定しようとするときに、ＥＭＤサービスセンタ１０２からＳＡＭ１０５$_1$～１０５$_4$に送信される。上述した第１の手法および第２の手法を採用する場合には、関連するコンテンツファイルＣＦ相互間と、コンテンツファイルＣＦとそれに対応するキーファイルＫＦとの間を、コンテンツファイルＣＦおよびキーファイルＫＦの少なくとも一方のヘッダに格納されたハイパーリンクデータを用いてリンク関係を確立する。ＳＡＭ１０５$_1$～１０５$_4$では、当該リンク関係に基づいて、コンテンツデータＣの権利処理および利用を行う。なお、本変形例において、コンテンツファイルＣＦおよびキーファイルＫＦのフォーマットは、例えば、図５（Ａ），（Ｂ）に示すものが採用される。また、この場合に、コンテンツファイルＣＦおよびキーファイルＫＦと共に、それらの署名データＳＩＧ$_{6,cp}$，ＳＩＧ$_{7,cp}$を送信することが好ましい。

第１実施形態の第５変形例

上述した実施形態では、セキュアコンテナ１０４内において、コンテンツファイルＣＦおよびキーファイルＫＦを別々に設けた場合を例示したが、例えば、図５３に示すように、セキュアコンテナ１０４内において、コンテンツファイルＣＦ内にキーファイルＫＦを格納するようにしてもよい。この場合に、キーファイルＫＦを格納したコンテンツファイルＣＦに対して、コンテンツプロバイダ１０１の秘密鍵データＫ$_{cp,s}$による署名データが付される。

第１実施形態の第６変形例

上述した実施形態では、コンテンツデータＣをコンテンツファイルＣＦに格納し、コンテンツ鍵データＫｃおよび権利書データ１０６をキーファイルＫＦ内に格納してコンテンップロバイダ１０１からＳＡＭ１０５$_1$などに送信する場合を例示したが、コンテンツデータＣ、コンテンツ鍵データＫｃおよび権利書データ１０６の少なくとも一つをファイル形式を採用せずにコンテンツプロバイダ１０１からＳＡＭ１０５$_1$などに、通信プロトコルに依存しない形式で送信してもよい。

【０２９６】例えば、図５４に示すように、コンテンツプロバイダ１０１において、コンテンツ鍵データＫｃで暗号化されたコンテンツデータＣと、暗号化されたコンテンツ鍵データＫｃおよび暗号化された権利書データ１０６などを含むキーファイルＫＦとを格納したセキュアコンテナ１０４ｓを作成し、セキュアコンテナ１０４ｓ

をＳＡＭ１０５$_1$などに通信プロトコルに依存しない形式で送信してもよい。

【０２９７】また、図５５に示すように、コンテンツプロバイダ１０１からＳＡＭ１０５$_1$などに、コンテンツ鍵データＫｃで暗号化されたコンテンツデータＣと、暗号化されたコンテンツ鍵データＫｃおよび暗号化された権利書データ１０６などを含むキーファイルＫＦとを通信プロトコルに依存しない形式で個別に送信してもよい。すなわち、コンテンツデータＣをファイル形式にしないで、キーファイルＫＦと同一経路で送信する。

【０２９８】また、図５６に示すように、コンテンツプロバイダ１０１からＳＡＭ１０５$_1$などに、コンテンツ鍵データＫｃで暗号化されたコンテンツデータＣを通信プロトコルに依存しない形式で送信すると共に、暗号化されたコンテンツ鍵データＫｃおよび暗号化された権利書データ１０６などを含むキーファイルＫＦをＥＭＤサービスセンタ１０２からＳＡＭ１０５$_1$などに送信してもよい。すなわち、コンテンツデータＣをファイル形式にしないで、キーファイルＫＦと別経路で送信する。

【０２９９】また、図５７に示すように、コンテンツプロバイダ１０１からＳＡＭ１０５$_1$などに、コンテンツ鍵データＫｃで暗号化されたコンテンツデータＣと、コンテンツ鍵データＫｃおよび権利書データ１０６とを、通信プロトコルに依存しない形式で送信してもよい。すなわち、コンテンツデータＣ、コンテンツ鍵データＫｃおよび権利書データ１０６をファイル形式にしないで、同一経路で送信する。

【０３００】また、図５８に示すように、コンテンツプロバイダ１０１からＳＡＭ１０５$_1$などに、コンテンツ鍵データＫｃで暗号化されたコンテンツデータＣを、通信プロトコルに依存しない形式で送信すると共に、ＥＭＤサービスセンタ１０２からＳＡＭ１０５$_1$などにコンテンツ鍵データＫｃおよび権利書データ１０６を送信してもよい。すなわち、コンテンツデータＣ、コンテンツ鍵データＫｃおよび権利書データ１０６をファイル形式にしないで、別経路で送信する。

【０３０１】第２実施形態

上述した実施形態では、コンテンツプロバイダ１０１からユーザホームネットワーク１０３のＳＡＭ１０５$_1$～１０５$_4$にコンテンツデータを直接配給する場合を例示したが、本実施形態では、コンテンツプロバイダが提供するコンテンツデータを、サービスプロバイダを介してユーザホームネットワークのＳＡＭに配給する場合について説明する。

【０３０２】図５９は、本実施形態のＥＭＤシステム３００の構成図である。図５９に示すように、ＥＭＤシステム３００は、コンテンツプロバイダ３０１、ＥＭＤサービスセンタ３０２、ユーザホームネットワーク３０３、サービスプロバイダ３１０、ペイメントゲートウェイ９０および決済機関９１を有する。コンテンツプロバイダ３０１、ＥＭＤサービスセンタ３０２、ＳＡＭ３０５$_1$～３０５$_4$およびサービスプロバイダ３１０は、それぞれ請求項２２などに係わるデータ提供装置、管理装置、データ処理装置およびデータ配給装置に対応している。コンテンツプロバイダ３０１は、サービスプロバイダ３１０に対してコンテンツデータを供給する点を除いて、前述した第１実施形態のコンテンツプロバイダ１０１と同じである。また、ＥＭＤサービスセンタ３０２は、コンテンツプロバイダ１０１およびＳＡＭ５０５$_1$～５０５$_4$に加えて、サービスプロバイダ３１０に対しても認証機能、鍵データ管理機能および権利処理機能を有する点を除いて、前述した第１実施形態のＥＭＤサービスセンタ１０２と同じである。また、ユーザホームネットワーク３０３は、ネットワーク機器３６０$_1$およびＡＶ機器３６０$_2$～３６０$_4$を有している。ネットワーク機器３６０$_1$はＳＡＭ３０５$_1$およびＣＡモジュール３１１を内蔵しており、ＡＶ機器３６０$_2$～３６０$_4$はそれぞれＳＡＭ３０５$_2$～３０５$_4$を内蔵している。ここで、ＳＡＭ３０５$_1$～３０５$_4$は、サービスプロバイダ３１０からセキュアコンテナ３０４の配給を受ける点と、コンテンツプロバイダ３０１に加えてサービスプロバイダ３１０についての署名データの検証処理およびＳＰ用購入履歴データ（データ配給装置用購入履歴データ）３０９の作成を行なう点とを除いて、前述した第１実施形態のＳＡＭ１０５$_1$～１０５$_4$と同じである。

【０３０３】先ず、ＥＭＤシステム３００の概要について説明する。ＥＭＤシステム３００では、コンテンツプロバイダ３０１は、自らが提供しようとするコンテンツのコンテンツデータＣの使用許諾条件などの権利内容を示す前述した第１実施形態と同様の権利書（ＵＣＰ：Ｕｓａｇｅ　ＣｏｎｔｒｏｌＰｏｌｉｃｙ）データ１０６およびコンテンツ鍵データＫｃを、高い信頼性のある権威機関であるＥＭＤサービスセンタ３０２に送信する。権利書データ１０６およびコンテンツ鍵データＫｃは、ＥＭＤサービスセンタ３０２に登録されて権威化（認証）される。

【０３０４】また、コンテンツプロバイダ３０１は、コンテンツ鍵データＫｃでコンテンツデータＣを暗号化してコンテンツファイルＣＦを生成する。また、コンテンツプロバイダ３０１は、ＥＭＤサービスセンタ３０２から、各コンテンツファイルＣＦについて、それぞれ６か月分のキーファイルＫＦを受信する。当該キーファイルＫＦ内には、当該キーファイルＫＦの改竄の有無、当該キーファイルＫＦの作成者および送信者の正当性を検証するための署名データが格納されている。そして、コンテンツプロバイダ３０１は、コンテンツファイルＣＦ、キーファイルＫＦおよび自らの署名データとを格納した図５に示すセキュアコンテナ１０４を、インターネットなどのネットワーク、デジタル放送、記録媒体あるいは非公式なプロトコルを用いてあるいはオフラインなどで

サービスプロバイダ３１０に供給する。また、セキュアコンテナ１０４に格納された署名データは、対応するデータの改竄の有無、当該データの作成者および送信者の正当性を検証するために用いられる。

【０３０５】サービスプロバイダ３１０は、コンテンツプロバイダ３０１からセキュアコンテナ１０４を受け取ると、署名データの検証を行なって、セキュアコンテナ１０４の作成者および送信者の確認する。次に、サービスプロバイダ３１０は、例えばオフラインで通知されたコンテンツプロバイダ３０１が希望するコンテンツに対しての価格（ＳＲＰ）に、自らが行ったオーサリングなどのサービスに対しての価格を加算した価格を示すプライスタグデータ（ＰＴ）３１２を作成する。そして、サービスプロバイダ３１０は、セキュアコンテナ１０４から取り出したコンテンツファイルＣＦおよびキーファイルＫＦと、プライスタグデータ３１２と、これらに対しての自らの秘密鍵データ$K_{SP.S}$による署名データとを格納したセキュアコンテナ３０４を作成する。このとき、キーファイルＫＦは、配信用鍵データKD_1～KD_6によって暗号化されており、サービスプロバイダ３１０は当該配信用鍵データKD_1～KD_6を保持していないため、サービスプロバイダ３１０はキーファイルＫＦの中身を見たり、書き換えたりすることはできない。また、ＥＭＤサービスセンタ３０２は、プライスタグデータ３１２を登録して権威化する。

【０３０６】サービスプロバイダ３１０は、オンラインおよび／またはオフラインでセキュアコンテナ３０４をユーザホームネットワーク３０３に配給する。このとき、オフラインの場合には、セキュアコンテナ３０４はＲＯＭ型の記録媒体などに記録されてＳＡＭ3051～3054にそのまま供給される。一方、オンラインの場合には、サービスプロバイダ３１０とＣＡモジュール３１１との間で相互認証を行い、セキュアコンテナ３０４をサービスプロバイダ３１０においてセッション鍵データK_{SES}を用いた暗号化して送信し、ＣＡモジュール３１１において受信したセキュアコンテナ３０４をセッション鍵データK_{SES}を用いて復号した後に、ＳＡＭ3051～3054に転送する。この場合に、コンテンツプロバイダ３０１からユーザホームネットワーク３０３にセキュアコンテナ３０４を送信する通信プロコトルとして、デジタル放送であればＭＨＥＧ（Ｍｕｌｔｉｍｅｄｉａ ａｎｄ Ｈｙｐｅｒｍｅｄｉａ ｉｎｆｏｒｍａｔｉｏｎ ｃｏｄｉｎｇ Ｅｘｐｅｒｔｓ Ｇｒｏｕｐ）プロトコルが用いられ、インターネットであればＸＭＬ／ＳＭＩＬ／ＨＴＭＬ（ＨｙｐｅｒＴｅｘｔＭａｒｋｕｐ Ｌａｎｇｕａｇｅ）が用いられ、これらの通信プロトコル内に、セキュアコンテナ３０４が、当該通信プロトコル（符号化方式など）に依存しない形式でトンネリングして埋め込まれる。従って、通信プロコトルとセキュアコンテナ３０４との間でフォーマットの整合性をとる必要性はなく、セキュアコンテナ３０４のフォーマットを柔軟に設定できる。

【０３０７】次に、ＳＡＭ3051～3054において、セキュアコンテナ３０４内に格納された署名データを検証して、セキュアコンテナ３０４に格納されたコンテンツファイルＣＦおよびキーファイルＫＦの作成者および送信者の正当性を確認する。そして、ＳＡＭ3051～3054において、当該正当性が確認されると、ＥＭＤサービスセンタ３０２から配給された対応する期間の配信用鍵データKD_1～KD_3を用いてキーファイルＫＦを復号する。ＳＡＭ3051～3054に供給されたセキュアコンテナ３０４は、ネットワーク機器3601およびＡＶ機器3602～3604において、ユーザの操作に応じて購入・利用形態が決定された後に、再生や記録媒体への記録などの対象となる。ＳＡＭ3051～3054は、上述したセキュアコンテナ３０４の購入・利用の履歴を利用履歴（Ｕｓａｇｅ Ｌｏｇ）データ３０８として記録する。利用履歴データ（履歴データまたは管理装置用履歴データ）３０８は、例えば、ＥＭＤサービスセンタ３０２からの要求に応じて、ユーザホームネットワーク３０３からＥＭＤサービスセンタ３０２に送信される。また、ＳＡＭ3051～3054は、コンテンツの購入形態が決定されると、当該購入形態を示す利用制御状態データ（ＵＣＳ：Ｕｓａｇｅ ｃｏｎｔｒｏｌｓｔａｔｅ Ｄａｔａ）１６６をＥＭＤサービスセンタ３０２に送信する。

【０３０８】ＥＭＤサービスセンタ３０２は、利用履歴データ３０８に基づいて、コンテンツプロバイダ３０１およびサービスプロバイダ３１０の各々について、課金内容を決定（計算）し、その結果に基づいて、ペイメントゲートウェイ９０を介して銀行などの決済機関９１に決済を行なう。これにより、ユーザホームネットワーク１０３のユーザが支払った金銭が、ＥＭＤサービスセンタ１０２による決済処理によって、コンテンツプロバイダ１０１およびサービスプロバイダ３１０に分配される。

【０３０９】本実施形態では、ＥＭＤサービスセンタ３０２は、認証機能、鍵データ管理機能および権利処理（利益分配）機能を有している。すなわち、ＥＭＤサービスセンタ３０２は、中立の立場にある最高の権威機関であるルート認証局９２に対してのセカンド認証局（Ｓｅｃｏｎｄ Ｃｅｒｔｉｆｉｃａｔｅ Ａｕｔｈｏｒｉｔｙ）としての役割を果たし、コンテンツプロバイダ３０１、サービスプロバイダ３１０およびＳＡＭ3051～3054において署名データの検証処理に用いられる公開鍵データの公開鍵証明書データに、ＥＭＤサービスセンタ３０２の秘密鍵データによる署名を付けることで、当該公開鍵データの正当性を認証する。また、前述したように、コンテンツプロバイダ３０１の権利書データ１０６、コンテンツ鍵データＫｃおよびサービスプロ

バイダ３１０のプライスタグデータ３１２を登録して権威化することも、ＥＭＤサービスセンタ３０２の認証機能によるものである。また、ＥＭＤサービスセンタ３０２は、例えば、配信用鍵データKD_1～KD_6などの鍵データの管理を行なう鍵データ管理機能を有する。また、ＥＭＤサービスセンタ３０２は、コンテンツプロバイダ３０１が登録した権利書データ１０６とＳＡＭ３０$5_1$～ＳＡＭ３０$5_4$から入力した利用履歴データ３０８とサービスプロバイダ３１０が登録したプライスタグデータ３１２とに基づいて、ユーザホームネットワーク３０３のユーザによるコンテンツの購入・利用に対して決済を行い、ユーザが支払った金銭をコンテンツプロバイダ３０１およびサービスプロバイダ３１０に分配して支払う権利処理（利益分配）機能を有する。

【０３１０】以下、コンテンツプロバイダ３０１の各構成要素について詳細に説明する。

〔コンテンツプロバイダ３０１〕図６０は、コンテンツプロバイダ３０１の機能ブロック図であり、サービスプロバイダ３１０との間で送受信されるデータに関連するデータの流れが示されている。図６０に示すように、コンテンツプロバイダ３０１は、コンテンツマスタソースデータベース１１１、電子透かし情報付加部１１２、圧縮部１１３、暗号化部１１４、乱数発生部１１５、署名処理部１１７、セキュアコンテナ作成部１１８、セキュアコンテナデータベース１１８ａ、キーファイルデータベース１１８ｂ、記憶部１１９、相互認証部１２０、暗号化・復号部１２１、権利書データ作成部１２２、ＥＭＤサービスセンタ管理部１２５およびサービスプロバイダ管理部３２４を有する。

【０３１１】図６０において、図３と同一符号を付した構成要素は、前述した第１実施形態において図３および図４を参照しながら説明した同一符号の構成要素と同じである。すなわち、コンテンツプロバイダ３０１は、図３に示すＳＡＭ管理部１２４の代わりにサービスプロバイダ管理部３２４を設けた構成をしている。サービスプロバイダ管理部３２４は、セキュアコンテナ作成部１１８から入力した図５に示すセキュアコンテナ１０４を、オフラインおよび／またはオンラインで、図５９に示すサービスプロバイダ３１０に提供する。

【０３１２】サービスプロバイダ管理部３２４は、図５に示すセキュアコンテナ１０４をオンラインでサービスプロバイダ３１０に配信する場合には、暗号化・復号部１２１においてセッション鍵データK_{SES}を用いてセキュアコンテナ１０４を暗号化した後に、ネットワークを介してサービスプロバイダ３１０に配信する。

【０３１３】また、図４に示すしたコンテンツプロバイダ１０１内でのデータの流れは、コンテンツプロバイダ３０１にも同様に適用される。

【０３１４】以下、コンテンツプロバイダ３０１からサービスプロバイダ３１０にセキュアコンテナ１０４を送信する際の処理の流れを説明する。図６１および図６２は、コンテンツプロバイダ３０１からサービスプロバイダ３１０にセキュアコンテナ１０４を送信する際の処理の流れを示すフローチャートである。

ステップＣ１：コンテンツプロバイダ３０１とサービスプロバイダ３１０との間で相互認証を行う。

ステップＣ２：ステップＣ１の相互認証によって得られたセッション鍵データK_{SES}を、コンテンツプロバイダ３０１およびサービスプロバイダ３１０の間で共有する。

ステップＣ３：サービスプロバイダ３１０によって、コンテンツプロバイダ３０１が所有する（ＣＰ用）セキュアコンテナデータベース１１８ａにアクセスが行われる。

ステップＣ４：サービスプロバイダ３１０は、例えば、セキュアコンテナデータベース１１８ａにおいて一元的に管理されているコンテンツＩＤとメタデータとのリストを参照して自らの配信サービスに必要なセキュアコンテナ１０４を選択する。

【０３１５】ステップＣ５：コンテンツプロバイダ３０１は、ステップＣ４で選択したセキュアコンテナ１０４を、ステップＣ２で共有したセッション鍵データK_{SES}を用いて暗号化する。

ステップＣ６：コンテンツプロバイダ３０１は、ステップＣ５で得られたセキュアコンテナ１０４を、コンテンツプロバイダ用商品配送プロトコルに挿入する。

【０３１６】ステップＣ７：サービスプロバイダ３１０は、ダウンロードを行う。

ステップＣ８：サービスプロバイダ３１０は、コンテンツプロバイダ用商品配送プロトコルからセキュアコンテナ１０４を取り出す。

ステップＣ９：サービスプロバイダ３１０は、セキュアコンテナ１０４を、ステップＣ２で共有したセッション鍵データK_{SES}を用いて復号する。

ステップＣ１０：サービスプロバイダ３１０は、復号したセキュアコンテナ１０４に格納されている署名データを検証して、送信者の正当性を確認し、送信者が正当であることの確認を条件にステップＣ１１の処理を行う。

ステップＣ１１：サービスプロバイダ３１０は、セキュアコンテナ１０４を自らのセキュアコンテナデータベースに格納する。

【０３１７】〔サービスプロバイダ３１０〕サービスプロバイダ３１０は、コンテンツプロバイダ３０１から提供を受けたセキュアコンテナ１０４内のコンテンツファイルＣＦおよびキーファイルＫＦと、自らが生成したプライスタグデータ３１２とを格納したセキュアコンテナ３０４を作成し、ユーザホームネットワーク３０３のネットワーク機器３６$0_1$およびＡＶ機器３６$0_2$～３６$0_4$にセキュアコンテナ３０４をオンラインおよび／またはオフラインで配給する。サービスプロバイダ３１０

によるコンテンツ配給のサービス形態には、大きく分けて、独立型サービスと連動型サービスとがある。独立型サービスは、例えば、コンテンツを個別に配給するダウンロード専用のサービスである。また、連動型サービスは、番組、ＣＭ（広告）に連動してコンテンツを配給するサービスであり、例えば、ドラマ番組のストリーム内にドラマの主題歌や挿入歌のコンテンツが格納してある。ユーザは、ドラマ番組を見ているときに、そのストリーム中にある主題歌や挿入歌のコンテンツを購入できる。

【０３１８】図６３は、サービスプロバイダ３１０の機能ブロック図である。なお、図６３には、コンテンツプロバイダ３０１から供給を受けたセキュアコンテナ１０４を用いて作成したセキュアコンテナ３０４をユーザホームネットワーク３０３に供給する際のデータの流れが示されている。図６３に示すように、サービスプロバイダ３１０は、コンテンツプロバイダ管理部３５０、記憶部３５１、相互認証部３５２、暗号化・復号部３５３、署名処理部３５４、セキュアコンテナ作成部３５５、セキュアコンテナデータベース３５５ａ、プライスタグデータ作成部３５６、ユーザホームネットワーク管理部３５７、ＥＭＤサービスセンタ管理部３５８およびユーザ嗜好フィルタ生成部９２０を有する。

【０３１９】以下、コンテンツプロバイダ３０１から供給を受けたセキュアコンテナ１０４からセキュアコンテナ３０４を作成し、これをユーザホームネットワーク３０３に配給する際のサービスプロバイダ３１０内での処理の流れを図６３および図６４を参照しながら説明する。図６４は、コンテンツプロバイダ３０１からユーザホームネットワーク３０３にセキュアコンテナ３０４を配給する処理を説明するためのフローチャートである。＜ステップＤ１＞コンテンツプロバイダ管理部３５０は、オンラインおよび／またはオフラインで、コンテンツプロバイダ３０１から図５に示すセキュアコンテナ１０４の供給を受けてセキュアコンテナ１０４を記憶部３５１に書き込む。このとき、コンテンツプロバイダ管理部３５０は、オンラインの場合には、図６０に示す相互認証部１２０と図６３に示す相互認証部３５２との間の相互認証によって得られたセッション鍵データK_{SES}を用いて、セキュアコンテナ１０４を暗号化・復号部３５３において復号した後に、記憶部３５１に書き込む。なお、サービスプロバイダ３１０は、記憶部３５１とは別に、セキュアコンテナ１０４を格納するための専用のセキュアコンテナデータベースを有してもよい。

【０３２０】＜ステップＤ２＞次に、署名処理部３５４において、記憶部３５１に記憶されているセキュアコンテナ１０４の図５（Ｃ）に示す署名データ$SIG_{1,ESC}$記憶部３５１から読み出したＥＭＤサービスセンタ３０２の公開鍵データ$K_{ESC,P}$を用いて検証し、その正当性が認められた後に、図５（Ｃ）に示す公開鍵証明書データCER_{CP}から公開鍵データ$K_{CP,P}$を取り出す。次に、署名処理部３５４は、当該取り出した公開鍵データ$K_{CP,P}$を用いて、記憶部３５１に記憶されているセキュアコンテナ１０４の図５（Ａ），（Ｂ）に示す署名データ$SIG_{6,CP}$，$SIG_{7,CP}$の検証、すなわちコンテンツファイルＣＦの作成者および送信者と、キーファイルＫＦの送信者との正当性の検証を行う。また、署名処理部３５４は、記憶部３５１から読み出した公開鍵データ$K_{ESC,P}$を用いて、図５（Ｂ）に示すキーファイルＫＦに格納された署名データ$SIG_{K1,ESC}$の検証、すなわちキーファイルＫＦの作成者の正当性の検証を行う。このとき、署名データ$SIG_{K1,ESC}$の検証は、キーファイルＫＦがＥＭＤサービスセンタ３０２に登録されているか否かの検証も兼ねている。

【０３２１】＜ステップＤ３＞次に、セキュアコンテナ作成部３５５は、署名データ$SIG_{6,CP}$，$SIG_{7,CP}$，$SIG_{K1,ESC}$の正当性が確認されると、記憶部３５１からコンテンツファイルＣＦおよびその署名データ$SIG_{6,CP}$と、キーファイルＫＦおよびその署名データ$SIG_{7,CP}$と、サービスプロバイダ３１０の公開鍵証明書データCER_{SP}およびその署名データ$SIG_{61,ESC}$と、コンテンツプロバイダ３０１の公開鍵証明書データCER_{CP}およびその署名データ$SIG_{1,ESC}$とを読み出す。

【０３２２】また、プライスタグデータ作成部３５６は、例えばコンテンツプロバイダ３０１からオフラインで通知されたコンテンツプロバイダ３０１が要求するコンテンツに対しての価格に、自らのサービスの価格を加算した価格を示すプライスタグデータ３１２を作成し、記憶部３５１に記憶する。

【０３２３】また、署名処理部３５４は、コンテンツファイルＣＦ、キーファイルＫＦおよびプライスタグデータ３１２のハッシュ値をとり、サービスプロバイダ３１０の秘密鍵データ$K_{SP,P}$を用いて、署名データ$SIG_{62,SP}$，$SIG_{63,SP}$，$SIG_{64,SP}$を作成し、これをセキュアコンテナ作成部３５５に出力する。ここで、署名データ$SIG_{62,SP}$はコンテンツファイルＣＦの送信者の正当性を検証するために用いられ、署名データ$SIG_{63,SP}$はキーファイルＫＦの送信者の正当性を検証するために用いられ、署名データ$SIG_{64,SP}$はプライスタグデータ３１２の作成者および送信者の正当性を検証するために用いられる。

【０３２４】次に、セキュアコンテナ作成部３５５は、図６５（Ａ）～（Ｄ）に示すように、コンテンツファイルＣＦおよびその署名データ$SIG_{6,CP}$，$SIG_{62,SP}$と、キーファイルＫＦおよびその署名データ$SIG_{7,CP}$，$SIG_{63,ESC}$と、プライスタグデータ３１２およびその署名データ$SIG_{64,SP}$と、公開鍵証明書データCER_{SP}およびそ

129

の署名データＳＩＧ$_{S1}$，$_{ESC}$と、公開鍵証明書データＣＥＲ$_{CP}$およびその署名データＳＩＧ$_{1}$，$_{ESC}$とを格納したセキュアコンテナ３０４を作成し、セキュアコンテナデータベース３５５ａに格納する。セキュアコンテナデータベース３５５ａに格納されたセキュアコンテナ３０４は、例えば、コンテンツＩＤなどを用いてサービスプロバイダ３１０によって一元的に管理される。

【０３２５】＜ステップＤ４＞セキュアコンテナ作成部３５５は、ユーザホームネットワーク３０３からの要求に応じたセキュアコンテナ３０４をセキュアコンテナデータベース３５５ａから読み出してユーザホームネットワーク管理部３５７に出力する。このとき、セキュアコンテナ３０４は、複数のコンテンツファイルＣＦと、それらにそれぞれ対応した複数のキーファイルＫＦとを格納した複合コンテナであってもよい。例えば、単数のセキュアコンテナ３０４内に、それぞれ曲、ビデオクリップ、歌詞カード、ライナーノーツおよびジャケットに関する複数のコンテンツファイルＣＦを単数のセキュアコンテナ３０４に格納してもよい。これらの複数のコンテンツファイルＣＦなどは、ディレクトリー構造でセキュアコンテナ３０４内に格納してもよい。

【０３２６】また、セキュアコンテナ３０４は、デジタル放送で送信される場合には、ＭＨＥＧ（Ｍｕｌｔｉｍｅｄｉａ ａｎｄ Ｈｙｐｅｒｍｅｄｉａ ｉｎｆｏｒｍａｔｉｏｎ ｃｏｄｉｎｇ Ｅｘｐｅｒｔｓ Ｇｒｏｕｐ）プロトコルが用いられ、インターネットで送信される場合にはＸＭＬ／ＳＭＩＬ／ＨＴＭＬ（ＨｙｐｅｒＴｅｘｔＭａｒｋｕｐ Ｌａｎｇｕａｇｅ）プロトコルが用いられる。このとき、セキュアコンテナ３０４内のコンテンツファイルＣＦおよびキーファイルＫＦなどは、ＭＨＥＧおよびＨＴＭＬのプロトコルをトンネリングした符号化方式に依存しない形式で、サービスプロバイダ３１０とユーザホームネットワーク３０３との間で採用される通信プロトコル内の所定の階層に格納される。

【０３２７】例えば、セキュアコンテナ３０４をデジタル放送で送信する場合には、図６６に示すように、コンテンツファイルＣＦが、ＭＨＥＧオブジェクト（Ｏｂｊｅｃｔ）内のＭＨＥＧコンテンツデータとして格納される。また、ＭＨＥＧオブジェクトは、トランスポート層プロコトルにおいて、動画である場合にはＰＥＳ（Ｐａｃｋｅｔｉｚｅｄ Ｅｌｅｍｅｎｔａｒｙ Ｓｔｒｅａｍ）－Ｖｉｄｅｏに格納され、音声である場合にはＰＥＳ－Ａｕｄｉｏに格納され、静止画である場合にはＰｒｉｖａｔｅ－Ｄａｔａに格納される。また、図６７に示すように、キーファイルＫＦ、プライスタグデータ３１２および公開鍵証明書データＣＥＲ$_{CP}$，ＣＥＲ$_{SP}$は、トランスポート層プロトコルのＴＳ Ｐａｃｋｅｔ内のＥＣＭ（Ｅｎｔｉｔｌｅｍｅｎｔ ＣｏｎｔｒｏｌＭｅｓｓａｇｅ）に格納される。ここで、コンテンツファイルＣＦ、キーファイルＫＦ、プライスタグデータ３１２および公開鍵証明書データＣＥＲ$_{CP}$，ＣＥＲ$_{SP}$は、コンテンツファイルＣＦのヘッダ内のディレクトリ構造データＤＳＤ$_{1}$によって相互間のリンクが確立されている。

130

【０３２８】次に、ユーザホームネットワーク管理部３５７は、セキュアコンテナ３０４を、オフラインおよび／またはオンラインでユーザホームネットワーク３０３に供給する。ユーザホームネットワーク管理部３５７は、セキュアコンテナ３０４をオンラインでユーザホームネットワーク３０３のネットワーク機器３６０$_{1}$に配信する場合には、相互認証後に、暗号化・復号部３５２においてセッション鍵データＫ$_{SES}$を用いてセキュアコンテナ３０４を暗号化した後に、ネットワークを介してネットワーク機器３６０$_{1}$に配信する。

【０３２９】なお、ユーザホームネットワーク管理部３５７は、セキュアコンテナ３０４を例えば衛星などを介して放送する場合には、セキュアコンテナ３０４をスクランブル鍵データＫ$_{SCR}$を用いて暗号化する。また、スクランブル鍵データＫ$_{SCR}$をワーク鍵データＫ$_{W}$を暗号化し、ワーク鍵データＫ$_{W}$をマスタ鍵データＫ$_{M}$を用いて暗号化する。そして、ユーザホームネットワーク管理部３５７は、セキュアコンテナ３０４と共に、スクランブル鍵データＫ$_{SCR}$およびワーク鍵データＫ$_{W}$を、衛星を介してユーザホームネットワーク３０３に送信する。また、例えば、マスタ鍵データＫ$_{M}$を、ＩＣカードなどに記憶してオフラインでユーザホームネットワーク３０３に配給する。

【０３３０】また、ユーザホームネットワーク管理部３５７は、ユーザホームネットワーク３０３から、当該サービスプロバイダ３１０が配給したコンテンツデータＣに関してのＳＰ用購入履歴データ３０９を受信すると、これを記憶部３５１に書き込む。サービスプロバイダ３１０は、将来のサービス内容を決定する際に、ＳＰ用購入履歴データ３０９を参照する。また、ユーザ嗜好フィルタ生成部９２０は、ＳＰ用購入履歴データ３０９に基づいて、当該ＳＰ用購入履歴データ３０９を送信したＳＡＭ３０５$_{1}$～３０５$_{4}$のユーザの嗜好を分析してユーザ嗜好フィルタデータ９００を生成し、これをユーザホームネットワーク管理部３５７を介してユーザホームネットワーク３０３のＣＡモジュール３１１に送信する。

【０３３１】図６８には、サービスプロバイダ３１０内におけるＥＭＤサービスセンタ３０２との間の通信に関連するデータの流れが示されている。なお、以下に示す処理を行う前提として、サービスプロバイダ３１０の関係者は、例えば、自らの身分証明書および決済処理を行う銀行口座などを用いて、オフラインで、ＥＭＤサービスセンタ３０２に登録処理を行い、グローバルユニークな識別子ＳＰ＿ＩＤを得ている。識別子ＳＰ＿ＩＤは、記憶部３５１に記憶される。

131

【０３３２】先ず、サービスプロバイダ３１０が、ＥＭＤサービスセンタ３０２に、自らの秘密鍵データＫ$_{SP,S}$に対応する公開鍵データＫ$_{SP,S}$の正当性を証明する公開鍵証明書データＣＥＲ$_{SP}$を要求する場合の処理を図６８を参照しながら説明する。サービスプロバイダ３１０は、真性乱数発生器を用いて乱数を発生して秘密鍵データＫ$_{SP,S}$を生成し、当該秘密鍵データＫ$_{SP,S}$に対応する公開鍵データＫ$_{SP,P}$を作成して記憶部３５１に記憶する。ＥＭＤサービスセンタ管理部３５８、サービスプロバイダ３１０の識別子ＳＰ＿ＩＤおよび公開鍵データＫ$_{SP,P}$を記憶部３５１から読み出す。そして、ＥＭＤサービスセンタ管理部３５８は、識別子ＳＰ＿ＩＤおよび公開鍵データＫ$_{SP,P}$を、ＥＭＤサービスセンタ３０２に送信する。そして、ＥＭＤサービスセンタ管理部３４８は、当該登録に応じて、公開鍵証明書データＣＥＲ$_{SP}$およびその署名データＳＩＧ$_{61,ESC}$をＥＭＤサービスセンタ３０２から入力して記憶部３５１に書き込む。

【０３３３】次に、サービスプロバイダ３１０が、ＥＭＤサービスセンタ３０２にプライスタグデータ３１２を登録して権威化する場合の処理を図６８を参照して説明する。

【０３３４】この場合には、署名処理部３５４において、記憶部３５１から読み出したプライスタグデータ３１２およびグローバルユニークな識別子であるコンテンツＩＤを格納した図６９に示すモジュールＭｏｄ$_{103}$のハッシュ値が求められ、秘密鍵データＫ$_{SP,S}$を用いて署名データＳＩＧ$_{80,SP}$が生成される。また、記憶部３５１から公開鍵証明書データＣＥＲ$_{SP}$およびその署名データＳＩＧ$_{61,ESC}$が読み出される。そして、図６９に示すプライスタグ登録要求用モジュールＭｏｄ$_{102}$が、相互認証部３５２とＥＭＤサービスセンタ３０２との間の相互認証によって得られたセッション鍵データＫ$_{SES}$を用いて暗号化・復号部３５３において暗号化された後に、ＥＭＤサービスセンタ管理部３５８からＥＭＤサービスセンタ３０２に送信される。なお、モジュールＭｏｄ$_{102}$に、サービスプロバイダ３１０のグローバルユニークな識別子ＳＰ＿ＩＤを格納してもよい。

【０３３５】また、ＥＭＤサービスセンタ管理部３５８は、ＥＭＤサービスセンタ３０２から受信した決済レポートデータ３０７ｓを記憶部３５１に書き込む。

【０３３６】また、ＥＭＤサービスセンタ管理部３５８は、ＥＭＤサービスセンタ３０２から受信したマーケティング情報データ９０４を記憶部３５１に記憶する。マーケティング情報データ９０４は、サービスプロバイダ３１０が今後配給するコンテンツデータＣを決定する際に参考にされる。

【０３３７】〔ＥＭＤサービスセンタ３０２〕ＥＭＤサービスセンタ３０２は、前述したように、認証局（ＣＡ：Ｃｅｒｔｉｆｉｃａｔｅ　Ａｕｔｈｏｒｉｔｙ）、

132

鍵管理（Ｋｅｙ　Ｍａｎａｇｅｍｅｎｔ）局および権利処理（Ｒｉｇｈｔｓ　Ｃｌｅａｒｉｎｇ）局としての役割を果たす。図７０は、ＥＭＤサービスセンタ３０２の機能の構成図である。図７０に示すように、ＥＭＤサービスセンタ３０２は、鍵サーバ１４１、鍵データベース１４１ａ、ＫＦ作成部１５３、決済処理部４４２、署名処理部４４３、決算機関管理部１４４、証明書・権利書管理部４４５、権利書データベース４４５ａ、証明書データベース４４５ｂ、コンテンツプロバイダ管理部１４８、ＣＰデータベース１４８ａ、ＳＡＭ管理部１４９、ＳＡＭデータベース１４９ａ、相互認証部１５０、暗号化・復号部１５１、サービスプロバイダ管理部３９０、ＳＰデータベース３９０ａ、コンテンツＩＤ作成部８５１、ユーザ嗜好フィルタ生成部９０１およびマーケティング情報データ生成部９０２を有する。図７０において、図２３および図２４と同じ符号を付した機能ブロックは、第１実施形態で説明した同一符号の機能ブロックと略同じ機能を有している。

【０３３８】以下、図７０において、新たな符号を付した機能ブロックについて説明する。なお、図７０には、ＥＭＤサービスセンタ３０２内の機能ブロック相互間のデータの流れのうち、サービスプロバイダ３１０との間で送受信されるデータに関連するデータの流れが示されている。また、図７１には、ＥＭＤサービスセンタ３０２内の機能ブロック相互間のデータの流れのうち、コンテンツプロバイダ３０１との間で送受信されるデータに関連するデータの流れが示されている。また、図７２には、ＥＭＤサービスセンタ３０２内の機能ブロック相互間のデータの流れのうち、図５９に示すＳＡＭ３０５$_1$～３０５$_4$および決済機関９１との間で送受信されるデータに関連するデータの流れが示されている。

【０３３９】決算処理部４４２は、図７２に示すように、ＳＡＭ３０５$_1$～３０５$_4$から入力した利用履歴データ３０８と、証明書・権利書管理部４４５から入力した標準小売価格データＳＲＰおよびプライスタグデータ３１２に基づいて決済処理を行う。なお、この際に、決済処理部４４２は、サービスプロバイダ３１０によるダンピングの有無などを監視する。決済処理部４４２は、決済処理により、図７２に示すように、コンテンツプロバイダ３０１についての決済レポートデータ３０７ｃおよび決済請求権データ１５２ｃを作成し、これらをそれぞれコンテンツプロバイダ管理部１４８および決算機関管理部１４４に出力する。また、決済処理により、図７０および図７２に示すように、サービスプロバイダ３１０についての決済レポートデータ３０７ｓおよび決済請求権データ１５２ｓを作成し、これらをそれぞれサービスプロバイダ管理部３９０および決算機関管理部１４４に出力する。ここで、決済請求権データ１５２ｃ，１５２ｓは、当該データに基づいて、決済機関９１に金銭の

支払いを請求できる権威化されたデータである。

【０３４０】ここで、利用履歴データ３０８は、第１実施形態で説明した利用履歴データ１０８と同様に、セキュアコンテナ３０４に関連したラインセンス料の支払いを決定する際に用いられる。利用履歴データ３０８には、例えば、図７３に示すように、セキュアコンテナ３０４に格納されたコンテンツデータＣの識別子であるコンテンツＩＤ、セキュアコンテナ３０４に格納されたコンテンツデータＣを提供したコンテンツプロバイダ３０１の識別子ＣＰ＿ＩＤ、セキュアコンテナ３０４を配給したサービスプロバイダ３１０の識別子ＳＰ＿ＩＤ、コンテンツデータＣの信号諸元データ、セキュアコンテナ３０４内のコンテンツデータＣの圧縮方法、セキュアコンテナ３０４を記録した記録媒体の識別子Ｍｅｄｉａ＿ＩＤ、セキュアコンテナ３０４を配給を受けたＳＡＭ３０５$_1$～３０５$_4$の識別子ＳＡＭＩＤ、当該ＳＡＭ１０５$_1$～１０５$_4$のユーザのＵＳＥＲ＿ＩＤなどが記述されている。従って、ＥＭＤサービスセンタ３０２は、コンテンツプロバイダ３０１およびサービスプロバイダ３１０の所有者以外にも、例えば、圧縮方法や記録媒体などのライセンス所有者に、ユーザホームネットワーク３０３のユーザが支払った金銭を分配する必要がある場合には、予め決められた分配率表に基づいて各相手に支払う金額を決定し、当該決定に応じた決済レポートデータおよび決済請求権データを作成する。

【０３４１】証明書・権利書管理部４４５は、証明書データベース４４５ｂに登録されて権威化された公開鍵証明書データCER_{CP}、公開鍵証明書データCER_{SP}および公開鍵証明書データCER_{SAM1}～CER_{SAM2}などを読み出すと共に、権利書データベース４４５ａにコンテンツプロバイダ３０１の権利書データ１０６およびコンテンツ鍵データＫｃ、並びにサービスプロバイダ３１０のプライスタグデータ３１２などを登録して権威化する。このとき、証明書・権利書管理部４４５は、権利書データ１０６、コンテンツ鍵データＫｃおよびプライスタグデータ３１２などのハッシュ値をとり、秘密鍵データ$K_{ESC,S}$を用いた署名データを付して権威化証明書データを作成する。

【０３４２】コンテンツプロバイダ管理部１４８は、コンテンツプロバイダ１０１との間で通信する機能を有し、登録されているコンテンツプロバイダ１０１の識別子ＣＰＩＤなどを管理するＣＰデータベース１４８ａにアクセスできる。

【０３４３】ユーザ嗜好フィルタ生成部９０１は、利用履歴データ３０８に基づいて、当該利用履歴データ３０８を送信したＳＡＭ３０５$_1$～３０５$_4$のユーザの嗜好に応じたコンテンツデータＣを選択するためのユーザ嗜好フィルタデータ９０３を生成し、ユーザ嗜好フィルタデータ９０３をＳＡＭ管理部１４９を介して、当該利用履歴データ３０８を送信したＳＡＭ３０５$_1$～３０５$_4$に送信する。

【０３４４】マーケティング情報データ生成部９０２は、利用履歴データ３０８に基づいて、例えば、複数のサービスプロバイダ３１０によってユーザホームネットワーク１０３に配給されたコンテンツデータＣの全体の購入状況などを示すマーケティング情報データ９０４を生成し、これをサービスプロバイダ管理部３９０を介して、サービスプロバイダ３１０に送信する。サービスプロバイダ３１０は、マーケティング情報データ９０４を参考にして、今後提供するサービスの内容を決定する。

【０３４５】以下、ＥＭＤサービスセンタ３０２内での処理の流れを説明する。ＥＭＤサービスセンタ３０２からＳＡＭ３０５$_1$～３０５$_4$への配信用鍵データKD_1～KD_3の送信は、第１実施形態の場合と同様に行なわれる。

【０３４６】また、ＥＭＤサービスセンタ３０２がコンテンツプロバイダ３０１から、公開鍵証明書データの発行要求を受けた場合の処理は証明書・権利書管理部４４５が証明書データベース４４５ｂにアクセスする点を除いて、前述した第１実施形態と同じである。また、権利書データ１０６などを登録する処理も、証明書・権利書管理部４４５が権利書データベース４４５ａに当該データを格納する点を除いて前述した第１実施形態の場合と同様である。

【０３４７】次に、ＥＭＤサービスセンタ３０２がサービスプロバイダ３１０から、公開鍵証明書データの発行要求を受けた場合の処理を、図７０を参照しながら説明する。この場合に、サービスプロバイダ管理部３９０は、予めＥＭＤサービスセンタ３０２によって与えられたサービスプロバイダ３１０の識別子ＳＰ＿ＩＤ、公開鍵データ$K_{SP,P}$および署名データ$SIG_{70,SP}$をサービスプロバイダ３１０から受信すると、これらを、相互認証部１５０と図６３に示す相互認証部３５２と間の相互認証で得られたセッション鍵データK_{SES}を用いて復号する。そして、当該復号した署名データ$SIG_{70,SP}$の正当性を署名処理部４４３において確認した後に、識別子ＳＰ＿ＩＤおよび公開鍵データ$K_{SP,P}$に基づいて、当該公開鍵証明書データの発行要求を出したサービスプロバイダ３１０がＳＰデータベース３９０ａに登録されているか否かを確認する。そして、証明書・権利書管理部４４５は、当該サービスプロバイダ３１０の公開鍵証明書データCER_{SP}を証明書データベース４４５ｂから読み出してサービスプロバイダ管理部３９０に出力する。また、署名処理部４４３は、公開鍵証明書データCER_{SP}のハッシュ値をとり、ＥＭＤサービスセンタ３０２の秘密鍵データ$K_{ESC,S}$を用いて、署名データ$SIG_{61,ESC}$を作成し、これをサービスプロバイダ管理部３９０に出力する。そして、サービスプロバイダ管理部３９０は、公開鍵証明書データCER_{SP}およびその署名データＳＩ

135

G_{61}，E_{SC}を、相互認証部１５０と図６３に示す相互認証部３５２と間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、サービスプロバイダ３１０に送信する。

【０３４８】なお、ＥＭＤサービスセンタ３０２がＳＡＭ105_1～105_4から、公開鍵証明書データの発行要求を受けた場合の処理は、第１実施形態と同様である。また、ＥＭＤサービスセンタ３０２が、コンテンツプロバイダ３０１から権利書データ１０６およびコンテンツ鍵データＫｃの登録要求を受けた場合の処理も、第１実施形態と同様である。また、ＥＭＤサービスセンタ３０２が、コンテンツプロバイダ３０１から受信した登録用モジュールMod_2に応じてキーファイルＫＦを作成してコンテンツプロバイダ３０１に送信する処理も、第１実施形態と同様である。

【０３４９】次に、ＥＭＤサービスセンタ３０２が、サービスプロバイダ３１０からプライスタグデータ３１２の登録要求を受けた場合の処理を、図７０を参照しながら説明する。この場合には、サービスプロバイダ管理部３９０がサービスプロバイダ３１０から図６９に示すプライスタグ登録要求モジュールMod_{102}を受信すると、相互認証部１５０と図６３に示す相互認証部３５２と間の相互認証で得られたセッション鍵データK_{SES}を用いてプライスタグ登録要求モジュールMod_{102}を復号する。そして、当該復号したプライスタグ登録要求モジュールMod_{102}に格納された署名データ$SIG_{80,SP}$の正当性を署名処理部４４３において確認した後に、プライスタグ登録要求モジュールMod_{102}に格納されたプライスタグデータ３１２を、証明書・権利書管理部４４５を介して権利書データベース４４５ａに登録して権威化する。

【０３５０】次に、ＥＭＤサービスセンタ３０２において決済を行なう場合の処理を図７２を参照しながら説明する。ＳＡＭ管理部１４９は、ユーザホームネットワーク３０３の例えばＳＡＭ3051_1から利用履歴データ３０８およびその署名データ$SIG_{205,SAM1}$を入力すると、利用履歴データ３０８および署名データ$SIG_{205,SAM1}$を、相互認証部１５０とＳＡＭ3051_1～3054_4との間の相互認証によって得られたセッション鍵データK_{SES}を用いて復号し、ＳＡＭ3051_1の公開鍵データ$K_{SAM1,p}$を用いて署名データ$SIG_{205,SAM1}$の検証を行なった後に、決算処理部４４２に出力する。

【０３５１】そして、決済処理部４４２は、ＳＡＭ3051_1から入力した利用履歴データ３０８と、証明書・権利書管理部４４５から入力した標準小売価格データＳＲＰおよびプライスタグデータ３１２とに基づいて決済処理を行う。決済処理部４４２は、決済処理により、図７２に示すように、コンテンツプロバイダ３０１についての決済レポートデータ３０７ｃおよび決済請求権データ

136

１５２ｃを作成し、これらをそれぞれコンテンツプロバイダ管理部１４８および決算機関管理部１４４に出力する。また、決済処理により、図７０および図７２に示すように、サービスプロバイダ３１０についての決済レポートデータ３０７ｓおよび決済請求権データ１５２ｓを作成し、これらをそれぞれサービスプロバイダ管理部３９０および決算機関管理部１４４に出力する。

【０３５２】次に、決算機関管理部１４４は、決済請求権データ１５２ｃ，１５２ｓと、それらについて秘密鍵データ$K_{ESC,S}$を用いて作成した署名データとを、相互認証およびセッション鍵データK_{SES}による復号を行なった後に、図５９に示すペイメントゲートウェイ９０を介して決済機関９１に送信する。これにより、決済請求権データ１５２ｃに示される金額の金銭がコンテンツプロバイダ３０１に支払われ、決済請求権データ１５２ｓに示される金額の金銭がサービスプロバイダ３１０に支払われる。

【０３５３】次に、ＥＭＤサービスセンタ３０２がコンテンツプロバイダ３０１およびサービスプロバイダ３１０に決済レポートデータ３０７ｃおよび３０７ｓを送信する場合の処理を説明する。決算処理部４４２において決済が行なわれると、決算処理部４４２からコンテンツプロバイダ管理部１４８に決済レポートデータ３０７ｃが出力される。コンテンツプロバイダ管理部１４８は、決算処理部４４２から決済レポートデータ３０７ｃを入力すると、これを、相互認証部１５０と図６０に示す相互認証部１２０と間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、コンテンツプロバイダ３０１に送信する。また、決算処理部４４２において決済が行なわれると、決算処理部４４２からサービスプロバイダ管理部３９０に決済レポートデータ３０７ｓが出力される。サービスプロバイダ管理部３９０は、決算処理部４４２から決済レポートデータ３０７ｓを入力すると、これを、相互認証部１５０と図６３に示す相互認証部３５２と間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、サービスプロバイダ３１０に送信する。

【０３５４】ＥＭＤサービスセンタ３０２は、その他に、第１実施形態のＥＭＤサービスセンタ１０２と同様に、ＳＡＭ3051_1～3054_4の出荷時の処理と、ＳＡＭ登録リストの登録処理とを行なう。

【０３５５】〔ユーザホームネットワーク３０３〕ユーザホームネットワーク３０３は、図５９に示すように、ネットワーク機器3601_1およびＡ／Ｖ機器3602_2～3604_4を有している。ネットワーク機器3601_1は、ＣＡモジュール３１１およびＳＡＭ3051_1を内蔵している。また、ＡＶ機器3602_2～3604_4は、それぞれＳＡＭ3052_2～3054_4を内蔵している。ＳＡＭ3051_1～3054_4の相互間は、例えば、１３９４シリアルインタフェースバスなどのバス１９１を介して接続され

ている。なお、ＡＶ機器３６０$_2$～３６０$_4$は、ネットワーク通信機能を有していてもよいし、ネットワーク通信機能を有しておらず、バス１９１を介してネットワーク機器３６０$_1$のネットワーク通信機能を利用してもよい。また、ユーザホームネットワーク３０３は、ネットワーク機能を有していないＡＶ機器のみを有していてもよい。

【０３５６】以下、ネットワーク機器３６０$_1$について説明する。図７４は、ネットワーク機器３６０$_1$の構成図である。図７４に示すように、ネットワーク機器３６０$_1$は、通信モジュール１６２、ＣＡモジュール３１１、復号モジュール９０５、ＳＡＭ３０５$_1$、復号・伸長モジュール１６３、購入・利用形態決定操作部１６５、ダウンロードメモリ１６７、再生モジュール１６９および外部メモリ２０１を有する。図７４において、図２５と同一符号を付した構成要素は、第１実施形態で説明した同一符号の構成要素と同じである。

【０３５７】通信モジュール１６２は、サービスプロバイダ３１０との間の通信処理を行なう。具体的には、通信モジュール１６２は、サービスプロバイダ３１０から衛星放送などで受信したセキュアコンテナ３０４を復号モジュール９０５に出力する。また、通信モジュール１６２は、サービスプロバイダ３１０から電話回線などを介して受信したユーザ嗜好フィルタデータ９００をＣＡモジュール３１１に出力すると共に、ＣＡモジュール３１１から入力したＳＰ用購入履歴データ３０９を電話回線などを介してサービスプロバイダ３１０に送信する。

【０３５８】図７５は、ＣＡモジュール３１１および復号モジュール９０５の機能ブロック図である。図７５に示すように、ＣＡモジュール３１１は、相互認証部９０６、記憶部９０７、暗号化・復号部９０８およびＳＰ用購入履歴データ生成部９０９を有する。相互認証部９０６は、ＣＡモジュール３１１とサービスプロバイダ３１０との間で電話回線を介してデータを送受信する際に、サービスプロバイダ３１０との間で相互認証を行ってセッション鍵データK_{SES}生成し、これを暗号化・復号部９０８に出力する。

【０３５９】記憶部９０７は、例えば、サービスプロバイダ３１０とユーザとの間で契約が成立した後に、サービスプロバイダ３１０からＩＣカード９１２などを用いてオフラインで供給されたマスタ鍵データK_Mを記憶する。

【０３６０】暗号化・復号部９０８は、復号モジュール９０５の復号部９１０からそれぞれ暗号化されたスクランブル鍵データK_{SCR}およびワーク鍵データK_Wを入力し、記憶部９０７から読み出したマスタ鍵データK_Mを用いてワーク鍵データK_Wを復号する。そして、暗号化・復号部９０８は、当該復号したワーク鍵データK_Wを用いてスクランブル鍵データK_{SCR}を復号し、当該復号したスクランブル鍵データK_{SCR}を復号部９１０に出力する。また、暗号化・復号部９０８は、電話回線などを介して通信モジュール１６２がサービスプロバイダ３１０から受信したユーザ嗜好フィルタデータ９００を、相互認証部９０６からのセッション鍵データK_{SES}を用いて復号して復号モジュール９０５のセキュアコンテナ選択部９１１に出力する。また、暗号化・復号部９０８は、ＳＰ用購入履歴データ生成部９０９から入力したＳＰ用購入履歴データ３０９を、相互認証部９０６からのセッション鍵データK_{SES}用いて復号して通信モジュール１６２を介してサービスプロバイダ３１０に送信する。

【０３６１】ＳＰ用購入履歴データ生成部９０９は、図７４に示す購入・利用形態決定操作部１６５を用いてユーザによるコンテンツデータＣの購入操作に応じた操作信号Ｓ１６５、またはＳＡＭ３０５$_1$からの利用制御状態データ１６６に基づいて、サービスプロバイダ３１０に固有のコンテンツデータＣの購入履歴を示すＳＰ用購入履歴データ３０９を生成し、これを暗号化・復号部９０８に出力する。ＳＰ用購入履歴データ３０９は、例えば、サービスプロバイダ３１０が配信サービスに関してユーザから徴収したい情報、月々の基本料金（ネットワーク家賃）、契約（更新）情報および購入履歴情報などを含む。

【０３６２】なお、ＣＡモジュール３１１は、サービスプロバイダ３１０が課金機能を有している場合には、サービスプロバイダ３１０の課金データベース、顧客管理データベースおよびマーケティング情報データベースと通信を行う。この場合に、ＣＡモジュール３１１は、コンテンツデータの配信サービスについての課金データをサービスプロバイダ３１０に送信する。

【０３６３】復号モジュール９０５は、復号部９１０およびセキュアコンテナ選択部９１１を有する。復号部９１０は、通信モジュール１６２から、それぞれ暗号化されたセキュアコンテナ３０４、スクランブル鍵データK_{SCR}およびワーク鍵データK_Wを入力する。そして、復号部９１０は、暗号化されたスクランブル鍵データK_{SCR}およびワーク鍵データK_WをＣＡモジュール３１１の暗号化・復号部９０８に出力し、暗号化・復号部９０８から復号されたスクランブル鍵データK_{SCR}を入力する。そして、復号部９１０は、暗号化されたセキュアコンテナ３０４を、スクランブル鍵データK_{SCR}を用いて復号した後に、セキュアコンテナ選択部９１１に出力する。

【０３６４】なお、セキュアコンテナ３０４が、ＭＰＥＧ２ Ｔｒａｎｓｐｏｒｔ Ｓｔｒｅａｍ 方式でサービスプロバイダ３１０から送信される場合には、例えば、復号部９１０は、ＴＳ Ｐａｃｋｅｔ内のＥＣＭ（Ｅｎｔｉｔｌｅｍｅｎｔ Ｃｏｎｔｒｏｌ Ｍｅｓｓａｇｅ）からスクランブル鍵データK_{SCR}を取り出し、ＥＭＭ（Ｅｎｔｉｔｌｅｍｅｎｔ Ｍａｎａｇｅｍ

139

ｃｎｔ　Ｍｅｓｓａｇｅ）からワーク鍵データKwを取り出す。ＥＣＭには、その他に、例えば、チャンネル毎の番組属性情報などが含まれている。また、ＥＭＭは、その他に、ユーザ（視聴者）毎に異なる個別試聴契約情報などが含まれている。

【０３６５】セキュアコンテナ選択部９１１は、復号部９１０から入力したセキュアコンテナ３０４を、ＣＡモジュール３１１から入力したユーザ嗜好フィルタデータ９００を用いてフィルタリング処理して、ユーザの嗜好に応じたセキュアコンテナ３０４を選択してＳＡＭ３０５$_1$に出力する。

【０３６６】次に、ＳＡＭ３０５$_1$について説明する。なお、ＳＡＭ３０５$_1$は、サービスプロバイダ３１０についての署名検証処理を行なうなど、コンテンツプロバイダ３０１に加えてサービスプロバイダ３１０に関しての処理を行う点を除いて、図２６～図４１などを用いて前述した第１実施形態のＳＡＭ１０５$_1$と基本的に行なう機能および構造を有している。また、ＳＡＭ３０５$_2$～３０５$_4$は、ＳＡＭ３０５$_1$と基本的に同じ機能を有している。すなわち、ＳＡＭ３０５$_1$～３０５$_4$は、コンテンツ単位の課金処理をおこなうモジュールであり、ＥＭＤサービスセンタ３０２との間で通信を行う。

【０３６７】以下、ＳＡＭ３０５$_1$の機能について詳細に説明する。図７６は、ＳＡＭ３０５$_1$の機能の構成図である。なお、図７６には、サービスプロバイダ３１０からセキュアコンテナ３０４を入力する際の処理に関連するデータの流れが示されている。図７６に示すように、ＳＡＭ３０５$_1$は、相互認証部１７０、暗号化・復号部１７１，１７２，１７３、誤り訂正部１８１、ダウンロードメモリ管理部１８２、セキュアコンテナ復号部１８３、復号・伸長モジュール管理部１８４、ＥＭＤサービスセンタ管理部１８５、利用監視部１８６、署名処理部１８９、ＳＡＭ管理部１９０、記憶部１９２、メディアＳＡＭ管理部１９７、スタックメモリ２００、サービスプロバイダ管理部５８０、課金処理部５８７、署名処理部５９８および外部メモリ管理部８１１を有する。なお、図７６に示すＳＡＭ３０５$_1$の所定の機能は、ＳＡＭ１０５$_1$の場合と同様に、ＣＰＵにおいて秘密プログラムを実行することによって実現される。図７６において、図２６と同じ符号を付した機能ブロックは、第１実施形態で説明した同一符号の機能ブロックと同じである。

【０３６８】また、図７４に示す外部メモリ２０１には、第１実施形態で説明した処理および後述する処理を経て、利用履歴データ３０８およびＳＡＭ登録リストが記憶される。また、スタックメモリ２００には、図７７に示すように、コンテンツ鍵データＫｃ、権利書データ（ＵＣＰ）１０６、記憶部１９２のロック鍵データＫ$_{Loc}$、コンテンツプロバイダ３０１の公開鍵証明書データＣＥＲ$_{cp}$、サービスプロバイダ３１０の公開鍵証

140

明書データＣＥＲ$_{sp}$、利用制御状態データ（ＵＣＳ）３６６、ＳＡＭプログラム・ダウンロード・コンテナＳＤＣ$_1$～ＳＤＣ$_3$およびプライスタグデータ３１２などが記憶される。

【０３６９】以下、ＳＡＭ３０５$_1$の機能ブロックのうち、図７６において新たに符号を付した機能ブロックについて説明する。署名処理部５８９は、記憶部１９２あるいはスタックメモリ２００から読み出したＥＭＤサービスセンタ３０２の公開鍵データＫ$_{ESC,P}$、コンテンツプロバイダ３０１の公開鍵データＫ$_{cp,p}$およびサービスプロバイダ３１０の公開鍵データＫ$_{SP,P}$を用いて、セキュアコンテナ３０４内の署名データの検証を行なう。

【０３７０】課金処理部５８７は、図７８に示すように、図７４に示す購入・利用形態決定操作部１６５からの操作信号Ｓ１６５と、スタックメモリ２００から読み出されたプライスタグデータ３１２とに基づいて、ユーザによるコンテンツの購入・利用形態に応じた課金処理を行う。課金処理部５８７による課金処理は、利用監視部１８６の監視の下、権利書データ１０６が示す使用許諾条件などの権利内容および利用制御状態データ１６６に基づいて行われる。すなわち、ユーザは、当該権利内容などに従った範囲内でコンテンツの購入および利用を行うことができる。

【０３７１】また、課金処理部５８７は、課金処理において、利用履歴データ３０８を生成し、これを外部メモリ管理部８１１を介して外部メモリ２０１に書き込む。ここで、利用履歴データ３０８は、第１実施形態の利用履歴データ１０８と同様に、ＥＭＤサービスセンタ３０２において、セキュアコンテナ３０４に関連したラインセンス料の支払いを決定する際に用いられる。

【０３７２】また、課金処理部５８７は、操作信号Ｓ１６５に基づいて、ユーザによるコンテンツの購入・利用形態を記述した利用制御状態（ＵＣＳ：Ｕｓａｇｅ　Ｃｏｎｔｒｏｌ　Ｓｔａｔｕｓ）データ１６６を生成し、これをスタックメモリ２００に書き込む。コンテンツの購入形態としては、例えば、購入者による再生や当該購入者の利用のための複製に制限を加えない買い切りや、再生する度に課金を行なう再生課金などがある。ここで、利用制御状態データ１６６は、ユーザがコンテンツの購入形態を決定したときに生成され、以後、当該決定された購入形態で許諾された範囲内でユーザが当該コンテンツの利用を行なうように制御するために用いられる。利用制御状態データ１６６には、コンテンツのＩＤ、購入形態、買い切り価格、当該コンテンツの購入が行なわれたＳＡＭのＳＡＭ__ＩＤ，購入を行なったユーザのＵＳＥＲ__ＩＤなどが記述されている。

【０３７３】なお、決定された購入形態が再生課金である場合には、例えば、ＳＡＭ３０５$_1$からサービスプロバイダ３１０に利用制御状態データ１６６をリアルタイ

141

ムに送信し、サービスプロバイダ３１０がＥＭＤサービスセンタ３０２に、利用履歴データ３０８をＳＡＭ１０５$_1$に取りに行くことを指示する。また、決定された購入形態が買い切りである場合には、例えば、利用制御状態データ１６６が、サービスプロバイダ３１０およびＥＭＤサービスセンタ３０２にリアルタイムに送信される。

【０３７４】また、ＳＡＭ３０５$_1$では、図７６に示すように、ＥＭＤサービスセンタ管理部１８５を介してＥＭＤサービスセンタ３０２から受信したユーザ嗜好フィルタデータ９０３が、サービスプロバイダ管理部５８０に出力される。そして、サービスプロバイダ管理部５８０において、図７４に示す復号モジュール９０５から入力したセキュアコンテナ３０４のうち、ユーザ嗜好フィルタデータ９０３に基づいてフィルタリングされてユーザの嗜好に応じたセキュアコンテナ３０４が選択され、当該選択されたセキュアコンテナ３０４が誤り訂正部１８１に出力される。これにより、ＳＡＭ３０５$_1$において、当該ＳＡＭ３０５$_1$のユーザが契約している全てのサービスプロバイダ３１０を対象として、当該ユーザによるコンテンツデータＣの購入状況から得られた当該ユーザの嗜好に基づいたコンテンツデータＣの選択処理が可能になる。

【０３７５】以下、ＳＡＭ３０５$_1$内での処理の流れを説明する。ＥＭＤサービスセンタ３０２から受信した配信用鍵データＫＤ$_1$～ＫＤ$_3$を記憶部１９２に格納する際のＳＡＭ３０５$_1$内での処理の流れは、前述したＳＡＭ１０５$_1$の場合と同様である。

【０３７６】次に、セキュアコンテナ３０４をサービスプロバイダ３１０から入力する際のＳＡＭ３０５$_1$内での処理の流れを図７６を参照しながら説明する。相互認証部１７０と図６３に示すサービスプロバイダ３１０の相互認証部３５２との間で相互認証が行なわれる。暗号化・復号部１７１は、当該相互認証によって得られたセッション鍵データＫ$_{SES}$を用いて、サービスプロバイダ管理部５８０を介してサービスプロバイダ３１０から受信した図６５に示すセキュアコンテナ３０４を復号する。

【０３７７】次に、署名処理部５８９は、図６５（Ｄ）に示す署名データＳＩＧ$_{61,ESC}$，ＳＩＧ$_{1,ESC}$の検証を行った後に、公開鍵証明書データＣＥＲ$_{SP}$，ＣＥＲ$_{CP}$内に格納された公開鍵データＫ$_{SP,P}$，Ｋ$_{CP,P}$を用いて、署名データＳＩＧ$_{6,CP}$，ＳＩＧ$_{62,SP}$，ＳＩＧ$_{7,CP}$，ＳＩＧ$_{63,SP}$，ＳＩＧ$_{64,SP}$の正当性を検証する。ここで、署名データＳＩＧ$_{6,CP}$，ＳＩＧ$_{62,SP}$を検証することでコンテンツファイルＣＦの作成者および送信者の正当性が確認され、署名データＳＩＧ$_{7,CP}$，ＳＩＧ$_{63,SP}$を検証することでキーファイルＫＦの送信者の正当性が確認され、署名データＳＩＧ$_{64,SP}$を検証することでプライスタグデータ３１２の作成者および送信者の正当性が確認される。また、署名処理部５８９は、記憶部１９２から読み出した公開鍵データＫ$_{ESC,P}$を用いて、図６５（Ｂ）に示すキーファイルＫＦに格納された署名データＳＩＧ$_{K1,ESC}$の正当性を検証することで、キーファイルＫＦの作成者の正当性、並びにキーファイルＫＦがＥＭＤサービスセンタ３０２で登録されているか否かを検証する。

142

【０３７８】サービスプロバイダ管理部５８０は、署名処理部５８９において上述した全ての署名データの正当性が確認されると、セキュアコンテナ３０４を誤り訂正部１８１に出力する。

【０３７９】誤り訂正部１８１は、セキュアコンテナ３０４を誤り訂正した後に、ダウンロードメモリ管理部１８２に出力する。ダウンロードメモリ管理部１８２は、相互認証部１７０と図７４に示すメディアＳＡＭ１６７ａとの間で相互認証を行なった後に、セキュアコンテナ３０４をダウンロードメモリ１６７に書き込む。

【０３８０】次に、ダウンロードメモリ管理部１８２は、相互認証部１７０と図７４に示すメデイアＳＡＭ１６７ａとの間で相互認証を行なった後に、セキュアコンテナ３０４に格納された図６５（Ｂ）に示すキーファイルＫＦをダウンロードメモリ１６７から読み出してセキュアコンテナ復号部１８３に出力する。

【０３８１】そして、セキュアコンテナ復号部１８３は、記憶部１９２から入力した対応する期間の配信用鍵データＫＤ$_1$～ＫＤ$_3$を用いて、図６５（Ｂ）に示すキーファイルＫＦに格納されたコンテンツ鍵データＫｃ、権利書データ１０６およびＳＡＭプログラム・ダウンロード・コンテナＳＤＣ$_1$～ＳＤＣ$_3$が復号される。そして、復号されたコンテンツ鍵データＫｃ、権利書データ１０６およびＳＡＭプログラム・ダウンロード・コンテナＳＤＣ$_1$～ＳＤＣ$_3$がスタックメモリ２００に書き込まれる。

【０３８２】以下、サービスプロバイダ３１０からダウンロードメモリ１６７にダウンロードされたセキュアコンテナ３０４の購入形態を決定するまでの処理の流れを図７８および図７９を参照しながら説明する。図７９は、セキュアコンテナ３０４の購入形態決定処理を説明するためのフローチャートである。

＜ステップＥ１＞ユーザによる図７４に示す購入・利用形態決定操作部１６５の操作によって、試聴モードを示す操作信号Ｓ１６５が課金処理部５８７に出力された場合には、ステップＥ２の処理が行われ、そうでない場合にはステップＥ３の処理が行われる。

【０３８３】＜ステップＥ２＞試聴モードを示す操作信号Ｓ１６５が課金処理部５８７に出力された場合に行われ、例えば、ダウンロードメモリ１６７に記憶されているコンテンツファイルＣＦが、復号・伸長モジュール管

143

理部１８４を介して、図７４に示す復号・伸長モジュール１６３に出力される。このとき、コンテンツファイルＣＦに対して、相互認証部１７０とメディアＳＡＭ１６７ａとの間の相互認証およびセッション鍵データＫ$_{SES}$による暗号化・復号と、相互認証部１７０と相互認証部２２０との間の相互認証およびセッション鍵データＫ$_{SES}$による暗号化・復号とが行なわれる。コンテンツファイルＣＦは、図７４に示す復号部２２１においてセッション鍵データＫ$_{SES}$を用いて復号された後に、復号部２２２に出力される。

【０３８４】また、スタックメモリ２００から読み出されたコンテンツ鍵データＫｃおよび半開示パラメータデータ１９９が、図７４に示す復号・伸長モジュール１６３に出力される。このとき、相互認証部１７０と相互認証部２２０との間の相互認証後に、コンテンツ鍵データＫｃおよび半開示パラメータデータ１９９に対してセッション鍵データＫ$_{SES}$による暗号化および復号が行なわれる。次に、復号された半開示パラメータデータ１９９が半開示処理部２２５に出力され、半開示処理部２２５からの制御によって、復号部２２２によるコンテンツ鍵データＫｃを用いたコンテンツデータＣの復号が半開示で行われる。次に、半開示で復号されたコンテンツデータＣが、伸長部２２３において伸長された後に、電子透かし情報処理部２２４に出力される。次に、電子透かし情報処理部２２４においてユーザ電子透かし情報用データ１９６がコンテンツデータＣに埋め込まれた後、コンテンツデータＣが再生モジュール１６９において再生され、コンテンツデータＣに応じた音響が出力される。

【０３８５】＜ステップＥ３＞ユーザが、購入・利用形態決定操作部１６５を操作して購入形態を決定すると、当該決定した購入形態を示す操作信号Ｓ１６５が課金処理部１８７に出力される。

【０３８６】＜ステップＥ４＞課金処理部１８７において、決定された購入形態に応じた利用履歴データ３０８および利用制御状態データ１６６が生成され、利用履歴データ３０８が外部メモリ管理部８１１を介して外部メモリ２０１に書き込まれると共に利用制御状態データ１６６がスタックメモリ２００に書き込まれる。以後は、利用監視部１８６において、利用制御状態データ１６６によって許諾された範囲で、コンテンツの購入および利用が行なわれるように制御（監視）される。そして、スタックメモリ２００に格納されているキーファイルＫＦと、利用制御状態データ１６６とを用いて、購入形態が決定した後述する図８１（Ｃ）に示す新たなキーファイルＫＦ$_1$が生成され、当該作成されたキーファイルＫＦ$_1$がスタックメモリ２００にに記憶される。図８１（Ｃ）に示すように、キーファイルＫＦ$_1$に格納された利用制御状態データ１６６はストレージ鍵データＫ$_{STR}$およびメディア鍵データＫ$_{MED}$を用いてＤＥＳのＣＢＣモードを利用して順に暗号化されている。ここで、記録用鍵データＫ$_{STR}$は、例えばＳＡＣＤ（Ｓｕｐｅｒ　Ａｕｄｉｏ　Ｃｏｍｐａｃｔ　Ｄｉｓｃ）、ＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｃ）機器、ＣＤ－Ｒ機器およびＭＤ（Ｍｉｎｉ　Ｄｉｓｃ）機器などの種類に応じて決まるデータであり、機器の種類と記録媒体の種類とを１対１で対応づけるために用いられる。また、メディア鍵データＫ$_{MED}$は、記録媒体にユニークなデータである。

144

【０３８７】また、署名処理部５８９において、ＳＡＭ３０５$_1$の秘密鍵データＫ$_{SAM1,S}$を用いて、キーファイルＫＦ$_1$のハッシュ値Ｈ$_{K1}$が作成され、当該作成されたハッシュ値Ｈ$_{K1}$が、キーファイルＫＦ$_1$と対応付けられて、スタックメモリ２００に記憶される。

【０３８８】＜ステップＥ５＞ＳＡＭ３０５$_1$からＥＭＤサービスセンタ３０２に、利用制御状態データ１６６が送信される。当該利用制御状態データ１６６の送信は、ＳＡＭ３０５において、コンテンツデータの購入形態が決定される度に行われる。なお、ＳＡＭ３０５$_1$からＥＭＤサービスセンタ３０２への利用履歴データ３０８の送信は、例えば、例えば、１箇月などの所定の時間間隔で行われる。

【０３８９】次に、ダウンロードメモリ１６７に記憶されている購入形態が既に決定されたコンテンツデータＣを再生する場合の処理の流れを、図７８を参照しながら説明する。この場合には、利用監視部１８６の監視下で、操作信号Ｓ１６５に基づいて、ダウンロードメモリ１６７に記憶されているコンテンツファイルＣＦが、図７４に示す復号・伸長モジュール１６３に出力される。また、スタックメモリ２００から読み出されたコンテンツ鍵データＫｃが復号・伸長モジュール１６３に出力される。そして、復号・伸長モジュール１６３の復号部２２２において、コンテンツ鍵データＫｃを用いたコンテンツファイルＣＦの復号と、伸長部２２３による伸長処理とが行なわれ、再生モジュール１６９において、コンテンツデータＣが再生される。このとき、課金処理部５８７において、操作信号Ｓ１６５に応じて、外部メモリ２０１に記憶されている利用履歴データ３０８が更新される。利用履歴データ３０８は、秘密鍵データＫ$_{SAM1,S}$を用いて作成した署名データＳＩＧ$_{205,SAM1}$と共に、ＥＭＤサービスセンタ管理部１８５を介して、所定のタイミングで、ＥＭＤサービスセンタ３０２に送信される。

【０３９０】次に、図８０に示すように、例えば、ネットワーク機器３６０$_1$のダウンロードメモリ１６７にダウンロードされた既に購入形態が決定された図８１に示すセキュアコンテナ３０４ｘを、バス１９１を介して、ＡＶ機器３６０$_2$のＳＡＭ３０５$_2$に転送する場合のＳＡＭ３０５$_1$内での処理の流れを図８２を参照しながら説明する。ユーザは、購入・利用形態決定操作部１６５を操作して、ダウンロードメモリ１６７に記憶された所

定のコンテンツをＡＶ機器３６０$_2$に転送することを指示し、当該操作に応じた操作信号Ｓ１６５が、課金処理部５８７に出力される。これにより、課金処理部５８７は、操作信号Ｓ１６５に基づいて、スタックメモリ２００に記憶されている利用履歴データ３０８を更新する。

【０３９１】また、ダウンロードメモリ管理部１８２は、ダウンロードメモリ１６７から読み出した図８１（Ａ），（Ｂ），（Ｃ）に示すコンテンツファイルＣＦおよびキーファイルＫＦ，ＫＦ$_1$を署名処理部５８９およびＳＡＭ管理部１９０に出力する。そして、署名処理部５８９は、コンテンツファイルＣＦおよびキーファイルＫＦの署名データＳＩＧ$_{41,SAM1}$，ＳＩＧ$_{42,SAM1}$を作成すると共に、キーファイルＫＦ$_1$のハッシュ値Ｈ$_{K1}$を作成し、これらをＳＡＭ管理部１９０に出力する。また、ＳＡＭ管理部１９０は、図８１（Ｄ），（Ｅ）に示すプライスタグデータ３１２およびその署名データＳＩＧ$_{64,SP}$と、公開鍵証明書データＣＥＲ$_{CP}$およびその署名データＳＩＧ$_{1,ESC}$とをスタックメモリ２００から読み出す。また、ＳＡＭ管理部１９０は、図８１（Ｅ）に示す公開鍵証明書データＣＥＲ$_{SAM1}$およびその署名データＳＩＧ$_{22,ESC}$を記憶部１９２から読み出す。

【０３９２】次に、ＳＡＭ管理部１９０は、図８１に示すセキュアコンテナ３０４ｘを作成する。また、相互認証部１７０は、ＳＡＭ３０５$_2$との間で相互認証を行って得たセッション鍵データＫ$_{SES}$を暗号化・復号部１７１に出力する。ＳＡＭ管理部１９０は、図８１に示すセキュアコンテナ３０４ｘを、暗号化・復号部１７１において、セッション鍵データＫ$_{SES}$を用いて暗号化した後に、図８２に示すＡＶ機器３６０$_2$のＳＡＭ３０５$_2$に出力する。

【０３９３】以下、図８０に示すように、ＳＡＭ３０５$_1$から入力したセキュアコンテナ３０４ｘを、ＲＡＭ型などの記録媒体（メディア）に書き込む際のＳＡＭ３０５$_2$内での処理の流れを、図８３を参照しながら説明する。

【０３９４】この場合には、ＳＡＭ３０５$_2$のＳＡＭ管理部１９０は、図８３に示すように、図８１に示すセキュアコンテナ３０４ｘを、ネットワーク機器３６０$_1$のＳＡＭ３０５$_1$から入力する。そして、ＳＡＭ３０５$_1$の相互認証部１７０とＳＡＭ３０５$_2$の相互認証部１７０との間の相互認証が行われ、署名処理部５８９において、当該相互認証によって得られたセッション鍵データＫ$_{SES}$用いて、セキュアコンテナ３０４ｘの復号が行われる。次に、署名処理部５８９において、記憶部１９２から読み出した公開鍵データＫ$_{ESC,P}$を用いて、図８１（Ｅ）に示す署名データＳＩＧ$_{61,ESC}$，ＳＩＧ$_{1,ESC}$，ＳＩＧ$_{22,ESC}$の正当性を検証する。そして、署名データＳＩＧ$_{61,ESC}$，ＳＩＧ$_{1,ESC}$，ＳＩＧ$_{22,ESC}$の正当性が確認される

と、署名処理部５８９において、公開鍵証明書データＣＥＲ$_{SP}$，ＣＥＲ$_{CP}$，ＣＥＲ$_{SAM1}$に含まれる公開鍵データＫ$_{SP,P}$，Ｋ$_{CP,P}$，Ｋ$_{SAM1,P}$を用いて、図８１（Ａ）～（Ｄ）に示す署名データＳＩＧ$_{6,CP}$，ＳＩＧ$_{62,SP}$，ＳＩＧ$_{41,SAM1}$，ＳＩＧ$_{7,CP}$，ＳＩＧ$_{63,SP}$，ＳＩＧ$_{42,SAM1}$，ＳＩＧ$_{64,SP}$およびハッシュ値Ｈ$_{K1}$の正当性が検証される。そして、これらの署名データの正当性が確認されると、スタックメモリ２００に、キーファイルＫＦ，ＫＦ$_1$およびプライスタグデータ３１２が記憶される。また、コンテンツファイルＣＦが、ＳＡＭ管理部１９０から記録モジュール管理部８５５に出力される。そして、図８１（Ｃ）に示すキーファイルＫＦ$_1$に格納されたコンテンツ鍵データＫｃおよび利用制御状態データ１６６が、スタックメモリ２００から暗号化・復号部１７３に読み出され、暗号化・復号部１７３において、記憶部１９２から読み出した記録用鍵データＫ$_{STR}$、メディア鍵データＫ$_{MED}$および購入者鍵データＫ$_{PIN}$を用いて順に暗号化された後に記録モジュール管理部８５５に出力される。また、スタックメモリ２００から読み出されたキーファイルＫＦが、記録モジュール管理部８５５に出力される。そして、相互認証部１７０とＲＡＭ型の記録媒体１３０$_4$のメディアＳＡＭ１３３との間の相互認証を行った後に、コンテンツファイルＣＦがＲＡＭ型の記録媒体１３０$_4$のセキュアでないＲＡＭ領域１３４に記憶され、キーファイルＫＦ，ＫＦ$_1$およびプライスタグデータ３１２がセキュアＲＡＭ領域１３２に書き込まれる。なお、キーファイルＫＦ，ＫＦ$_1$およびプライスタグデータ３１２を、ＲＡＭ型の記録媒体１３０$_4$のメディアＳＡＭ１３３に記憶するようにしてもよい。

【０３９５】なお、ＳＡＭ３０５$_1$内での処理のうち、コンテンツの購入形態が未決定のＲＯＭ型の記録媒体の購入形態を決定する際のＡＶ機器３６０$_2$内での処理の流れ、ＡＶ機器３６０$_3$において購入形態が未決定のＲＯＭ型の記録媒体からセキュアコンテナ３０４を読み出してこれをＡＶ機器３６０$_2$に転送してＲＡＭ型の記録媒体に書き込む際の処理の流れは、サービスプロバイダ３１０の秘密鍵データを用いた署名データの署名データの検証を行なう点と、購入形態を決定したキーファイル内にプライスタグデータ３１２を格納する点を除いて、第１実施形態のＳＡＭ１０５$_1$の場合と同じである。

【０３９６】次に、図５９に示すＥＭＤシステム３００の全体動作について説明する。図８４および図８５は、ＥＭＤシステム３００の全体動作のフローチャートである。ここでは、サービスプロバイダ３１０からユーザホームネットワーク３０３にオンラインでセキュアコンテナ３０４を送信する場合を例示して説明する。なお、以下に示す処理の前提として、ＥＭＤサービスセンタ３０２へのコンテンツプロバイダ３０１、サービスプロバイ

147

ダ３１０およびＳＡＭ３０５$_1$～３０５$_4$の登録は既に終了しているものとする。

【０３９７】ステップＳ２１：ＥＭＤサービスセンタ３０２は、コンテンツプロバイダ３０１の公開鍵データＫ$_{CP,P}$の公開鍵証明書ＣＥＲ$_{CP}$を、自らの署名データＳＩＧ$_{1,ESC}$と共にコンテンツプロバイダ３０１に送信する。また、ＥＭＤサービスセンタ３０２は、コンテンツプロバイダ３０１の公開鍵データＫ$_{SP,P}$の公開鍵証明書ＣＥＲ$_{SP}$を、自らの署名データＳＩＧ$_{61,ESC}$と共にサービスプロバイダ３１０に送信する。また、ＥＭＤサービスセンタ３０２は、各々有効期限が１カ月の３カ月分の配信用鍵データＫＤ$_1$～ＫＤ$_3$をユーザホームネットワーク３０３のＳＡＭ３０５$_1$～３０５$_4$に送信する。

【０３９８】ステップＳ２２：コンテンツプロバイダ３０１は、相互認証を行った後に、図１８に示す登録用モジュールＭｏｄ$_2$を、ＥＭＤサービスセンタ３０２に送信する。そして、ＥＭＤサービスセンタ３０２は、所定の署名検証を行った後に、権利書データ１０６およびコンテンツ鍵データＫｃを登録して権威化する。また、ＥＭＤサービスセンタ３０２は、登録用モジュールＭｏｄ$_2$に応じた図５（Ｂ）に示す６カ月分のキーファイルＫＦを作成し、これをコンテンツプロバイダ３０１に送信する。

【０３９９】ステップＳ２３：コンテンツプロバイダ３０１は、図５（Ａ），（Ｂ）に示すコンテンツファイルＣＦおよびその署名データＳＩＧ$_{6,CP}$と、キーファイルＫＦおよびその署名データＳＩＧ$_{7,CP}$とを作成し、これらと図５（Ｃ）に示す公開鍵証明書データＣＥＲ$_{CP}$およびその署名データＳＩＧ$_{1,ESC}$とを格納したセキュアコンテナ１０４を、オンラインおよび／またはオフラインで、サービスプロバイダ３１０に提供する。

【０４００】ステップＳ２４：サービスプロバイダ３１０は、図５（Ｃ）に示す署名データＳＩＧ$_{1,ESC}$を検証した後に、公開鍵証明書データＣＥＲ$_{CP}$に格納された公開鍵データＫ$_{CP,P}$を用いて、図５（Ａ），（Ｂ）に示す署名データＳＩＧ$_{8,CP}$およびＳＩＧ$_{7,CP}$を検証して、セキュアコンテナ１０４が正当なコンテンツプロバイダ３０１から送信されたものであるかを確認する。

【０４０１】ステップＳ２５：サービスプロバイダ３１０は、プライスタグデータ３１２およびその署名データＳＩＧ$_{64,SP}$を作成し、これらを格納したを格納した図６５に示すセキュアコンテナ３０４を作成する。

【０４０２】ステップＳ２６：サービスプロバイダ３１０は、図６９に示すプライスタグ登録要求モジュールＭｏｄ$_{102}$を、ＥＭＤサービスセンタ３０２に送信する。そして、ＥＭＤサービスセンタ３０２は、所定の署名検証を行った後に、プライスタグデータ３１２を登録して権威化する。

148

【０４０３】ステップＳ２７：サービスプロバイダ３１０は、例えば、ユーザホームネットワーク３０３のＣＡモジュール３１１からの要求に応じて、ステップＳ２５で作成したセキュアコンテナ３０４を、オンラインあるいはオフラインで、図７４に示すネットワーク機器３６０$_1$の復号モジュール９０５に送信する。

【０４０４】ステップＳ２８：ＣＡモジュール３１１は、ＳＰ用購入履歴データ３０９を作成し、これを所定のタイミングで、サービスプロバイダ３１０に送信する。

【０４０５】ステップＳ２９：ＳＡＭ３０５$_1$～３０５$_4$のいずれかにおいて、図６５（Ｄ）に示す署名データＳＩＧ$_{61,ESC}$を検証した後に、公開鍵証明書データＣＥＲ$_{SP}$に格納された公開鍵データＫ$_{SP,P}$を用いて、図６５（Ａ），（Ｂ），（Ｃ）に示す署名データＳＩＧ$_{62,SP}$，ＳＩＧ$_{63,SP}$，ＳＩＧ$_{64,SP}$を検証して、セキュアコンテナ３０４内の所定のデータが正当なサービスプロバイダ３１０において作成および送信されたか否かを確認する。

【０４０６】ステップＳ３０：ＳＡＭ３０５$_1$～３０５$_4$のいずれかにおいて、図６５（Ｄ）に示す署名データＳＩＧ$_{1,ESC}$を検証した後に、公開鍵証明書データＣＥＲ$_{CP}$に格納された公開鍵データＫ$_{CP,P}$を用いて、図６５（Ａ），（Ｂ），（Ｃ）に示す署名データＳＩＧ$_{6,SP}$，ＳＩＧ$_{7,SP}$を検証して、セキュアコンテナ３０４内のコンテンツファイルＣＦが正当なコンテンツプロバイダ３０１において作成されたか否かと、キーファイルＫＦが正当なコンテンツプロバイダ３０１から送信されたか否かを確認する。また、ＳＡＭ３０５$_1$～３０５$_4$のいずれかにおいて、公開鍵データＫ$_{ESC,P}$を用いて、図６５（Ｂ）に示すキーファイルＫＦ内の署名データＳＩＧ$_{K1,ESC}$の正当性を検証することで、キーファイルＫＦが正当なＥＭＤサービスセンタ３０２によって作成されたか否かを確認する。

【０４０７】ステップＳ３１：ユーザが図７４の購入・利用形態決定操作部１６５を操作してコンテンツの購入・利用形態を決定する。

【０４０８】ステップＳ３２：ステップＳ３１において生成された操作信号Ｓ１６５に基づいて、ＳＡＭ３０５$_1$～３０５$_4$において、セキュアコンテナ３０４の利用履歴（Ｕｓａｇｅ　Ｌｏｇ）データ３０８が生成される。ＳＡＭ３０５$_1$～３０５$_4$からＥＭＤサービスセンタ３０２に、利用履歴データ３０８およびその署名データＳＩＧ$_{205,SAM1}$が送信される。また、購入形態が決定される度にリアルタイムに、ＳＡＭ３０５$_1$～３０５$_4$からＥＭＤサービスセンタ３０２に利用制御状態データ１６６が送信される。

【０４０９】ステップＳ３３：ＥＭＤサービスセンタ３０２は、利用履歴データ３０８に基づいて、コンテンツ

プロバイダ３０１およびサービスプロバイダ３１０の各々について、課金内容を決定（計算）し、その結果に基づいて、決済請求権データ１５２ｃ，１５２ｓを作成する。

【０４１０】ステップＳ３４：ＥＭＤサービスセンタ３０２は、ペイメントゲートウェイ９０を介して決済機関９１に、決済請求権データ１５２ｃ，１５２ｓを自らの署名データと共に送信し、これにより、ユーザホームネットワーク３０３のユーザが決済機関９１に支払った金銭が、コンテンツプロバイダ３０１およびサービスプロバイダ３１０の所有者に分配される。

【０４１１】以上説明したように、ＥＭＤシステム３００では、図５に示すフォーマットのセキュアコンテナ１０４をコンテンツプロバイダ３０１からサービスプロバイダ３１０に配給し、セキュアコンテナ１０４内のコンテンツファイルＣＦおよびキーファイルＫＦをそのまま格納したセキュアコンテナ３０４をサービスプロバイダ３１０からユーザホームネットワーク３０３に配給し、キーファイルＫＦについての処理をＳＡＭ305_1～305_4内で行う。また、キーファイルＫＦに格納されたコンテンツ鍵データＫｃおよび権利書データ１０６は、配信鍵データKD_1～KD_3を用いて暗号化されており、配信鍵データKD_1～KD_3を保持しているＳＡＭ305_1～305_4内でのみ復号される。そして、ＳＡＭ305_1～305_4では、耐タンパ性を有するモジュールであり、権利書データ１０６に記述されたコンテンツデータＣの取り扱い内容に基づいて、コンテンツデータＣの購入形態および利用形態が決定される。

【０４１２】従って、ＥＭＤシステム３００によれば、ユーザホームネットワーク３０３におけるコンテンツデータＣの購入および利用を、サービスプロバイダ３１０における処理とは無関係に、コンテンツプロバイダ１０１の関係者が作成した権利書データ１０６の内容に基づいて確実に行わせることができる。すなわち、ＥＭＤシステム３００によれば、権利書データ１０６をサービスプロバイダ３１０が管理できないようできる。そのため、ＥＭＤシステム３００によれば、異系列の複数のサービスプロバイダ３１０を介してユーザホームネットワーク３０３にコンテンツデータＣが配給された場合でも、ユーザホームネットワーク３０３における当該コンテンツデータＣについての権利処理を、コンテンツプロバイダ３０１が作成した共通の権利書データ１０６に基づいて行わせることができる。

【０４１３】また、ＥＭＤシステム３００では、セキュアコンテナ１０４，３０４内の各ファイルおよびデータについて、それらの作成者および送信者の正当性を示す署名データを格納していることから、サービスプロバイダ３１０およびＳＡＭ305_1～305_4において、それらの作成者および送信者の正当性、並びにそれらが改竄されていないか否かなどを確認できる。その結果、コンテンツデータＣの不正利用を効果的に回避できる。

【０４１４】また、ＥＭＤシステム３００では、サービスプロバイダ３１０からユーザホームネットワーク１０３へのコンテンツデータＣの配給を、オンラインおよびオフラインの何れの場合でもセキュアコンテナ３０４を用いて行うことで、双方の場合において、ＳＡＭ3051～3054におけるコンテンツデータＣの権利処理を共通化できる。

【０４１５】また、ＥＭＤシステム３００では、ユーザホームネットワーク３０３内のネットワーク機器3601およびＡＶ機器3602～3604においてコンテンツデータＣを購入、利用、記録および転送する際に、常に権利書データ１０６に基づいて処理を行うことで、共通の権利処理ルールを採用できる。例えば、図８６に示すように、コンテンツプロバイダ３０１が提供したコンテンツデータＣを、サービスプロバイダ３１０からユーザホームネットワーク３０３に、パッケージ流通、デジタル放送、インターネット、専用線、デジタルラジオおよびモバイル通信などの何れの手法（経路）で配信（配給）した場合でも、ユーザホームネットワーク３０３，３０３ａのＳＡＭにおいて、コンテンツプロバイダ３０１が作成した権利書データ１０６に基づいて、共通の権利処理ルールが採用される。

【０４１６】また、ＥＭＤシステム３００によれば、ＥＭＤサービスセンタ３０２が、認証機能、鍵データ管理機能および権利処理（利益分配）機能を有することから、コンテンツの利用に伴ってユーザが支払った金額が、コンテンツプロバイダ３０１およびＥＭＤサービスセンタ３０２の所有者に、予め決められた比率に従って確実に分配される。また、ＥＭＤシステム３００によれば、同じコンテンツプロバイダ３０１が供給した同じコンテンツファイルＣＦについての権利書データ１０６は、サービスプロバイダ３１０のサービス形態とは無関係に、そのままＳＡＭ3051～3054に供給される。従って、ＳＡＭ3051～3054において、権利書データ１０６に基づいて、コンテンツプロバイダ３０１の意向通りに、コンテンツファイルＣＦの利用を行わせることができる。すなわち、ＥＭＤシステム３００によれば、コンテンツを用いたサービスおよびユーザによるコンテンツの利用が行われる際に、従来のように監査組織７２５に頼ることなく、技術的な手段によって、コンテンツプロバイダ３０１の所有者の権利および利益を確実に守ることができる。

【０４１７】以下、上述した第２実施形態のＥＭＤシステム３００で採用するセキュアコンテナなどの配送プロトコルの具体例について説明する。図８７に示すように、コンテンツプロバイダ３０１において作成されたセキュアコンテナ１０４は、インターネット（ＴＣＰ／ＩＰ）あるいは専用線（ＡＴＭＣｅｌｌ）などのコンテンツプロバイダ用配送プロトコルを用いてサービスプロバ

イダ３１０に提供される。また、サービスプロバイダ３１０は、セキュアコンテナ１０４を用いて作成したセキュアコンテナ３０４を、ディジタル放送（ＭＰＥＧ－ＴＳ上のＸＭＬ／ＳＭＩＬ）、インターネット（ＴＣＰ／ＩＰ上のＸＭＬ／ＳＭＩＬ）あるいはパッケージ流通（記録媒体）などのサービスプロバイダ用配送プロトコルを用いてユーザホームネットワーク３０３に配給する。また、ユーザホームネットワーク３０３，３０３ａ内、あるいはユーザホームネットワーク３０３と３０３ａとの間において、ＳＡＭ相互間で、セキュアコンテナが、家庭内ＥＣ／配信サービス（１３９４シリアルバス・インターフェイス上のＸＭＬ／ＳＭＩＬ）や記録媒体などを用いて転送される。

【０４１８】以下、図８７において、符号Ａ～Ｇを用いた経路におけるデータ転送に採用される配送プロトコルの一例を詳細に説明する。図８８は、図８７に示すコンテンツプロバイダ３０１とサービスプロバイダ３１０との間（符号Ａ）でセキュアコンテナ１０４などを配送するときに採用される配送プロトコルを説明するための図である。図８８に示すように、コンテンツプロバイダ３０１からサービスプロバイダ３１０にセキュアコンテナ１０４などが、ＩＰ／ＩＰ－ＳＥＣ層、ＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔｓ　Ｌａｙｅｒ）層、ＸＭＬ（ｅＸｔｅｎｓｉｂｌｅ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ）／ＳＭＩＬ（Ｓｙｎｃｈｒｏｎｉｚｅｄ　Ｍｕｌｔｉｍｅｄｉａ　Ｉｎｔｅｇｒａｔｉｏｎ　Ｌａｎｇｕａｇｅ）層およびアプリケーション層において共通鍵を用いたセッションを行って配送される。

【０４１９】図８９は、図８７に示すＥＭＤサービスセンタ３０２とコンテンツプロバイダ３０１との間（符号Ｂ）でキーファイルなどを配送するときに採用される配送プロトコルを説明するための図である。図８９に示すように、ＥＭＤサービスセンタ３０２からコンテンツプロバイダ３０１にキーファイルなどが、ＩＰ／ＩＰ－ＳＥＣ層、ＳＳＬ層およびアプリケーション層において共通鍵を用いたセッションを行って配送される。

【０４２０】図９０は、図に示すＥＭＤサービスセンタ３０２とサービスプロバイダ３１０との間（符号Ｃ）でプライスタグデータ３１２などを配送するときに採用される配送プロトコルを説明するための図である。図９０に示すように、ＥＭＤサービスセンタ３０２からサービスプロバイダ３１０にプライスタグデータ３１２などが、ＩＰ／ＩＰ－ＳＥＣ層、ＳＳＬ層およびアプリケーション層において共通鍵を用いたセッションを行って配送される。

【０４２１】図９１は、図８７に示すサービスプロバイダ３１０とユーザホームネットワーク３０３との間（符号Ｄ）、ユーザホームネットワーク３０３内（符号Ｅ）で、セキュアコンテナ３０４などを配送するときに採用される配送プロトコルを説明するための図である。図９１に示すように、サービスプロバイダ３１０からユーザホームネットワーク３０３のネットワーク機器３６０_1にセキュアコンテナ３０４などが配送される。このとき、サービスプロバイダ３１０とネットワーク機器３６０_1との間では、ＭＰＥＧ－ＴＳ層、ＰＥＳ層またはＤＳＭ＿ＣＣ＿Ｄａｔａ＿Ｃａｒｏｕｓｅｌ層、および、ＭＨＥＧ（Ｍｕｌｔｉｍｅｄｉａ　ａｎｄ　Ｈｙｐｅｒｍｅｄｉａ　Ｅｘｐｅｒｔｓ）層または「ｈｔｔｐ層およびＸＭＬ／ＳＭＩＬ層」が、セキュアコンテナ３０４を転送するためのサービスプロバイダ用商品配送プロトコルとして用いられる。また、ネットワーク機器３６０_1とストレージ機器３６０_2との間、並びにＡＶ機器相互間では、ＨＡＶｉ（ＸＭＬ）が、セキュアコンテナを転送するためのユーザホームネットワーク商品配送プロトコルとして用いられる。このとき、デジタル放送のデータ放送方式にＸＭＬ／ＳＭＩＬ／ＢＭＬを利用した場合には、セキュアコンテナ３０４のコンテンツファイルＣＦ１，ＣＦ２およびキーファイルＫＦ１，ＫＦ２と視聴（デモ）サンプルは、図９２に示すようにＨＴＴＰ層上のＢＭＬ／ＸＭＬ／ＳＭＩＬ層およびモノメディアデータ層に格納されて配送される。また、デジタル放送のデータ放送方式にＭＨＥＧを利用した場合には、セキュアコンテナ３０４のコンテンツファイルＣＦ１，ＣＦ２およびキーファイルＫＦ１，ＫＦ２と視聴（デモ）サンプルは、図９３に示すようにＭＨＥＧ層上のモノメディアデータ層に格納されて配送される。また、デジタル放送のデータ放送方式にＸＭＬ／ＳＭＩＬを利用した場合には、セキュアコンテナ３０４のコンテンツファイルＣＦ１，ＣＦ２およびキーファイルＫＦ１，ＫＦ２と視聴（デモ）サンプルは、図９４に示すようにＨＴＴＰ層上のＸＭＬ／ＳＭＩＬ層に格納されて配送される。

【０４２２】図９５は、図８７に示すＥＭＤサービスセンタ３０２とユーザホームネットワーク３０３，３０３ａとの間（符号Ｇ）で、利用履歴データ３０８および利用制御状態データ１６６などを配送するときに採用される配送プロトコルを説明するための図である。図９５に示すように、ネットワーク機器３６０_1からＥＭＤサービスセンタ３０２に、利用履歴データ３０８などが転送される場合に、ＩＰ／ＩＰ－ＳＥＣ層、ＳＳＬ層およびアプリケーション層において、セッション鍵データを用いたセッションが行われる。また、ネットワーク機器３６０_2などがＥＭＤサービスセンタ３０２に利用履歴データ３０８および利用制御状態データ１６６などを転送する場合には、利用履歴データ３０８などが、ＩＰ／ＩＰ－ＳＥＣ層およびＨＡＶｉ層でセッションを行ってストレージ機器３６０_2からネットワーク機器３６０_1に転送された後に、ネットワーク機器３６０_1からＥＭＤサービスセンタ３０２に前述したように転送される。

【０４２３】図９６は、図８７に示すユーザホームネットワーク３０３のストレージ機器３６０_4からユーザホ

ームネットワーク３０３ａのストレージ機器３６０$_{11}$に、セキュアコンテナを配送するときに採用される配送プロトコルを説明するための図である。図９６に示すように、ストレージ機器３６０$_4$からストレージ機器３６０$_{11}$にセキュアコンテナが、ＩＰ／ＩＰ－ＳＥＣ層、ＳＳＬ層、ＸＭＬ／ＳＭＩＬ層およびアプリケーション層において共通鍵を用いたセッションを行って配送される。

【０４２４】第２実施形態の第１変形例

図９７は、第２実施形態の第１変形例に係わる２個のサービスプロバイダを用いたＥＭＤシステム３００ａの構成図である。図９７において、図５９と同一符号を付した構成要素は、第１実施形態で説明した同一符号の構成要素と同じである。図９７に示すように、ＥＭＤシステム３００ａでは、コンテンツプロバイダ３０１からサービスプロバイダ３１０ａおよび３１０ｂに、同じセキュアコンテナ１０４を供給する。

【０４２５】サービスプロバイダ３１０ａは、例えば、コンテンツをドラマ番組の提供サービスを行っており、当該サービスにおいて、当該ドラマ番組に関連するコンテンツデータＣと、当該コンテンツデータＣについて独自に作成したプライスタグデータ３１２ａとを格納したセキュアコンテナ３０４ａを作成し、これをネットワーク機器３６０$_1$に配給する。また、サービスプロバイダ３１０ｂは、例えば、カラオケサービスを提供しており、当該サービスにおいて、当該カラオケサービスに関連するコンテンツデータＣと、当該コンテンツデータＣについて独自に作成したプライスタグデータ３１２ｂとを格納したセキュアコンテナ３０４ｂを作成し、これをネットワーク機器３６０$_1$に配給する。ここで、セキュアコンテナ３０４ａ，３０４ｂのフォーマットは、図６５を用いた説明したセキュアコンテナ３０４と同じである。

【０４２６】ネットワーク機器３６０ａ$_1$には、サービスプロバイダ３１０ａ，３１０ｂの各々に対応したＣＡモジュール３１１ａ，３１１ｂが設けられている。ＣＡモジュール３１１ａ，３１１ｂは、自らの要求に応じたセキュアコンテナ３０４ａ，３０４ｂの配給を、それぞれサービスプロバイダ３１０ａ，３１０ｂから受ける。

【０４２７】次に、ＣＡモジュール３１１ａ，３１１ｂは、配給されたセキュアコンテナ３０４ａ，３０４ｂに応じたＳＰ用購入履歴データ３０９ａ，３０９ｂをそれぞれ作成し、これらをそれぞれサービスプロバイダ３１０ａ，３１０ｂに送信する。また、ＣＡモジュール３１１ａ，３１１ｂは、セキュアコンテナ３０４ａ，３０４ｂをセッション鍵データK_{SES}で復号した後に、ＳＡＭ３０５$_1$～３０５$_4$に出力する。

【０４２８】次に、ＳＡＭ３０５$_1$～３０５$_4$において、共通の配信用鍵データKD_1～KD_3を用いて、セキュアコンテナ３０４ａ，３０４ｂ内のキーファイルＫＦが復号され、共通の権利書データ１０６に基づいて、ユーザからの操作に応じたコンテンツの購入・利用に関する処理が行われ、それに応じた利用履歴データ３０８が作成される。

【０４２９】そして、ＳＡＭ３０５$_1$～３０５$_4$からＥＭＤサービスセンタ３０２に、利用履歴データ３０８が送信される。

【０４３０】ＥＭＤサービスセンタ３０２では、利用履歴データ３０８に基づいて、コンテンツプロバイダ３０１およびサービスプロバイダ３１０ａ，３１０ｂの各々について、課金内容を決定（計算）し、その結果に基づいて、それぞれに対応する決済請求権データ１５２ｃ，１５２ｓａ，１５２ｓｂを作成する。

【０４３１】ＥＭＤサービスセンタ３０２は、ペイメントゲートウェイ９０を介して決済機関９１に、決済請求権データ１５２ｃ，１５２ｓａ，１５２ｓｂを送信し、これにより、ユーザホームネットワーク３０３のユーザが決済機関９１に支払った金銭が、コンテンツプロバイダ３０１およびサービスプロバイダ３１０ａ，３１０ｂの所有者に分配される。

【０４３２】上述したように、ＥＭＤシステム３００ａによれば、同じコンテンツファイルＣＦをサービスプロバイダに３１０ａ，３１０ｂに供給する場合に、当該コンテンツファイルＣＦについての権利書データ１０６を配信用鍵データKD_1～KD_6で暗号化してサービスプロバイダに３１０ａ，３１０ｂに供給し、サービスプロバイダに３１０ａ，３１０ｂは暗号化された権利書データ１０６をそのまま格納したセキュアコンテナ３０４ａ，３０４ｂをユーザホームネットワークに配給する。そのため、ユーザホームネットワーク内のＳＡＭ３０５$_1$～３０５$_4$では、コンテンツファイルＣＦをサービスプロバイダに３１０ａ，３１０ｂの何れから配給を受けた場合でも、共通の権利書データ１０６に基づいて権利処理を行うことができる。

【０４３３】なお、上述した第１変形例では、２個のサービスプロバイダを用いた場合を例示したが、本発明では、サービスプロバイダの数は任意である。

【０４３４】第２実施形態の第２変形例

図９８は、第２実施形態の第２変形例に係わる複数のコンテンツプロバイダを用いたＥＭＤシステム３００ｂの構成図である。図９８において、図５９と同一符号を付した構成要素は、第１実施形態で説明した同一符号の構成要素と同じである。図９８に示すように、ＥＭＤシステム３００ｂでは、ＥＭＤサービスセンタ３０２からコンテンツプロバイダ３０１ａ，３０１ｂにそれぞれキーファイルＫＦａ，ＫＦｂが供給され、コンテンツプロバイダ３０１ａ，３０１ｂからサービスプロバイダ３１０に、それぞれセキュアコンテナ１０４ａ，１０４ｂが供給される。

【０４３５】サービスプロバイダ３１０は、例えば、コ

ンテンツプロバイダ３０１ａ，３０１ｂが供給したコンテンツを用いてサービスを提供しており、セキュアコンテナ１０４ａについてのプライスタグデータ３１２ａと、セキュアコンテナ１０４ｂについてのプライスタグデータ３１２ｂとをそれぞれ生成し、これらを格納したセキュアコンテナ３０４ｃを作成する。図９８に示すように、セキュアコンテナ３０４ｃには、コンテンツファイルＣＦａ，ＣＦｂ、キーファイルＫＦａ，ＫＦｂ、プライスタグデータ３１２ａ，３１２ｂ、それらの各々についてのサービスプロバイダ３１０の秘密鍵データＫｃｐ，ｓによる署名データが格納されている。

【０４３６】セキュアコンテナ３０４ｃは、ユーザホームネットワーク３０３のネットワーク機器３６０ｉのＣＡモジュール３１１で受信された後に、ＳＡＭ３０５ｉ～３０５ｋにおいて処理される。

【０４３７】ＳＡＭ３０５ｉ～３０５ｋでは、配信用鍵データＫＤａｉ～ＫＤａｓを用いて、キーファイルＫＦａが復号され、権利書データ１０６ａに基づいて、コンテンツファイルＣＦａについてのユーザからの操作に応じた購入・利用に関する処理が行われ、その履歴が利用履歴データ３０８に記述される。また、ＳＡＭ３０５ｉ～３０５ｋにおいて、配信用鍵データＫＤｂｉ～ＫＤｂｓを用いて、キーファイルＫＦｂが復号され、権利書データ１０６ｂに基づいて、コンテンツファイルＣＦｂについてのユーザからの操作に応じた購入・利用に関する処理が行われ、その履歴が利用履歴データ３０８に記述される。

【０４３８】そして、ＳＡＭ３０５ｉ～３０５ｋからＥＭＤサービスセンタ３０２に、利用履歴データ３０８が送信される。

【０４３９】ＥＭＤサービスセンタ３０２では、利用履歴データ３０８に基づいて、コンテンツプロバイダ３０１ａ，３０１ｂおよびサービスプロバイダ３１０の各々について、課金内容を決定（計算）し、その結果に基づいて、それぞれに対応する決済請求権データ１５２ｃａ，１５２ｃｂ，１５２ｓを作成する。

【０４４０】ＥＭＤサービスセンタ３０２は、ペイメントゲートウェイ９０を介して決済機関９１に、決済請求権データ１５２ｃａ，１５２ｃｂ，１５２ｓを送信し、これにより、ユーザホームネットワーク３０３のユーザが決済機関９１に支払った金銭が、コンテンツプロバイダ３０１ａ，３０１ｂおよびサービスプロバイダ３１０の所有者に分配される。

【０４４１】上述したように、ＥＭＤシステム３００ｂによれば、セキュアコンテナ３０４ｃ内に格納されたコンテンツファイルＣＦａ，ＣＦｂの権利書データ１０６ａ，１０６ｂは、コンテンツプロバイダ３０１ａ，３０１ｂが作成したものをそのまま用いるため、ＳＡＭ３０５ｉ～３０５ｋ内において、権利書データ１０６ａ，１０６ｂに基づいて、コンテンツファイルＣＦａ，ＣＦｂについての権利処理がコンテンツプロバイダ３０１ａ，３０１ｂの意向に沿って確実に行われる。

【０４４２】なお、図９８に示す第２変形例では、２個のコンテンツプロバイダを用いた場合を例示したが、コンテンツプロバイダの数は任意である。また、コンテンツプロバイダおよびサービスプロバイダの双方が複数であってもよい。

【０４４３】第２実施形態の第３変形例

図９９は、第２実施形態の第３変形例に係わるＥＭＤシステムの構成図である。上述した第２実施形態では、ＥＭＤサービスセンタ３０２が決済機関９１に対して、コンテンツプロバイダ３０１およびサービスプロバイダ３１０の決済を行う場合を例示したが、本発明では、例えば、図９９に示すように、ＥＭＤサービスセンタ３０２において、利用履歴データ３０８に基づいて、コンテンツプロバイダ３０１のための決済請求権データ１５２ｃと、サービスプロバイダ３１０のための決済請求権データ１５２ｓとを作成し、これらをそれぞれコンテンツプロバイダ３０１およびサービスプロバイダ３１０に送信するようにしてもよい。この場合には、コンテンツプロバイダ３０１は、決済請求権データ１５２ｃを用いて、ペイメントゲートウェイ９０ａを介して決済機関９１ａに決済を行う。また、サービスプロバイダ３１０は、決済請求権データ１５２ｓを用いて、ペイメントゲートウェイ９０ｂを介して決済機関９１ｂに決済を行う。

【０４４４】第２実施形態の第４変形例

図１００は、第２実施形態の第４変形例に係わるＥＭＤシステムの構成図である。上述した第２実施形態では、例えば現行のインターネットのようにサービスプロバイダ３１０が課金機能を有していない場合を例示したが、現行のデジタル放送などのようにサービスプロバイダ３１０が課金機能を有している場合には、ＣＡモジュール３１１において、セキュアコンテナ３０４に関するサービスプロバイダ３１０のサービスに対しての利用履歴データ３０８ｓを作成してサービスプロバイダ３１０に送信する。そして、サービスプロバイダ３１０は、利用履歴データ３０８ｓに基づいて、課金処理を行って決済請求権データ１５２ｓを作成し、これを用いてペイメントゲートウェイ９０ｂを介して決済機関９１ｂに決済を行う。一方、ＳＡＭ３０５ｉ～３０５ｋは、セキュアコンテナ３０４に関するコンテンツプロバイダ３０１の権利処理に対しての利用履歴データ３０８ｃを作成し、これをＥＭＤサービスセンタ３０２に送信する。ＥＭＤサービスセンタ３０２は、利用履歴データ３０８ｃに基づいて、決済請求権データ１５２ｃを作成し、これをコンテンツプロバイダ３０１に送信する。コンテンツプロバイダ３０１は、決済請求権データ１５２ｃを用いて、ペイメントゲートウェイ９０ａを介して決済機関９１ａに決済を行う。

【０４４５】第２実施形態の第５変形例

157

上述した実施形態では、図７２に示すように、ＥＭＤサービスセンタ３０２のユーザ嗜好フィルタ生成部９０１において、ＳＡＭ３０５$_1$などから受信した利用履歴データ３０８に基づいて、ユーザ嗜好フィルタデータ９０３を生成する場合を例示したが、例えば、図７８に示すＳＡＭ３０５$_1$などの利用監視部１８６で生成されてリアルタイムにＥＭＤサービスセンタ３０２に送信された利用制御状態データ１６６に基づいて、ユーザ嗜好フィルタ生成部９０１においてユーザ嗜好フィルタデータ９０３を生成してもよい。

【０４４６】第２実施形態の第６変形例

コンテンツプロバイダ３０１、サービスプロバイダ３１０およびＳＡＭ３０５$_1$～３０５$_4$は、それぞれ自らの公開鍵データ$K_{CP,P}$，$K_{SP,P}$，$K_{SAM1,P}$～$K_{SAM4,P}$の他に、自らの秘密鍵データ$K_{CP,S}$，$K_{SP,S}$，$K_{SAM1,S}$～$K_{SAM4,S}$をＥＭＤサービスセンタ３０２に登録してもよい。このようにすることで、ＥＭＤサービスセンタ３０２は、緊急時に、国家あるいは警察機関などからの要請に応じて、秘密鍵データ$K_{CP,S}$，$K_{SP,S}$，$K_{SAM1,S}$～$K_{SAM4,S}$を用いて、コンテンツプロバイダ３０１とサービスプロバイダ３１０との間の通信、サービスプロバイダ３１０とＳＡＭ３０５$_1$～３０５$_4$との間の通信、並びにユーザホームネットワーク３０３内でのＳＡＭ３０５$_1$～３０５$_4$相互間での通信のうち対象となる通信を盗聴することが可能になる。また、ＳＡＭ３０５$_1$～３０５$_4$については、出荷時に、ＥＭＤサービスセンタ３０２によって秘密鍵データ$K_{SAM1,S}$～$K_{SAM4,S}$を生成し、これをＳＡＭ３０５$_1$～３０５$_4$に格納すると共にＥＭＤサービスセンタ３０２が保持（登録）するようにしてもよい。

【０４４７】第２実施形態の第７変形例

上述した実施形態では、コンテンツプロバイダ３０１，サービスプロバイダ３１０およびＳＡＭ３０５$_1$～３０５$_4$が、相互に通信を行う場合に、ＥＭＤサービスセンタ３０２から事前に公開鍵証明書データ$CERC_P$，$CERS_P$，$CERS_{AM1}$～$CERS_{AN4}$を取得し、イン・バンド方式で通信先に送信する場合を例示したが、本発明では、通信先への公開鍵証明書データの送信形態として種々の形態を採用できる。例えば、コンテンツプロバイダ３０１，サービスプロバイダ３１０およびＳＡＭ３０５$_1$～３０５$_4$が、相互に通信を行う場合に、ＥＭＤサービスセンタ３０２から事前に公開鍵証明書データ$CERC_P$，$CERS_P$，$CERS_{AM1}$～$CERS_{AN4}$を取得し、当該通信に先立ってアウト・オブ・バンド方式で通信先に送信してもよい。また、コンテンツプロバイダ３０１、サービスプロバイダ３１０およびＳＡＭ３０５$_1$～３０５$_4$が、通信時に、ＥＭＤサービスセンタ３０２から公開鍵証明書データ$CERC_P$，$CERS_P$，$CERS_{AM1}$～$CERS_{AN4}$を取得してもよい。

158

【０４４８】図１０１は、公開鍵証明書データの取得（入手）ルートの形態を説明するための図である。なお、図１０１において、図５９と同じ符号を付した構成要素は、前述した同一符号の構成要素と同じである。また、ユーザホームネットワーク３０３ａは、前述したユーザホームネットワーク３０３と同じである。ユーザホームネットワーク３０３ｂでは、ＩＥＥＥ１３９４シリアルバスであるバス１９１を介してＳＡＭ３０５$_{11}$～３０５$_{14}$を接続している。

【０４４９】コンテンツプロバイダ３０１がサービスプロバイダ３１０の公開鍵証明書データ$CERS_P$を取得する場合には、例えば、通信に先立ってサービスプロバイダ３１０からコンテンツプロバイダ３０１に公開鍵証明書データ$CERS_P$を送信する場合（図１０１中（３））と、コンテンツプロバイダ３０１がＥＭＤサービスセンタ３０２から公開鍵証明書データ$CERS_P$を取り寄せる場合（図１０１中（１））とがある。

【０４５０】また、サービスプロバイダ３１０がコンテンツプロバイダ３０１の公開鍵証明書データ$CERC_P$を取得する場合には、例えば、通信に先立ってコンテンツプロバイダ３０１からサービスプロバイダ３１０に公開鍵証明書データ$CERC_P$を送信する場合（図１０１中（２））と、サービスプロバイダ３１０がＥＭＤサービスセンタ３０２から公開鍵証明書データ$CERC_P$を取り寄せる場合（図１０１中（４））とがある。

【０４５１】また、サービスプロバイダ３１０がＳＡＭ３０５$_1$～３０５$_4$の公開鍵証明書データ$CERS_{AM1}$～$CERS_{AM4}$を取得する場合には、例えば、通信に先立ってＳＡＭ３０５$_1$～３０５$_4$からサービスプロバイダ３１０に公開鍵証明書データ$CERS_{AM1}$～$CERS_{AM4}$を送信する場合（図１０１中（６））と、サービスプロバイダ３１０がＥＭＤサービスセンタ３０２から公開鍵証明書データ$CERS_{AM1}$～$CERS_{AM4}$を取り寄せる場合（図１０１中（４））とがある。

【０４５２】また、ＳＡＭ３０５$_1$～３０５$_4$がサービスプロバイダ３１０の公開鍵証明書データ$CERS_P$を取得する場合には、例えば、通信に先立ってサービスプロバイダ３１０からＳＡＭ３０５$_1$～３０５$_4$に公開鍵証明書データ$CERS_P$を送信する場合（図１０１中（５））と、ＳＡＭ３０５$_1$～３０５$_4$がＥＭＤサービスセンタ３０２から公開鍵証明書データ$CERS_P$を取り寄せる場合（図１０１中（７）など）とがある。

【０４５３】また、ＳＡＭ３０５$_1$がＳＡＭ３０５$_2$の公開鍵証明書データ$CERS_{AM2}$を取得する場合には、例えば、通信に先立ってＳＡＭ３０５$_2$からＳＡＭ３０５$_1$に公開鍵証明書データ$CERS_{AM2}$を送信する場合（図１０１中（８））と、ＳＡＭ３０５$_1$がＥＭＤサービスセンタ３０２から公開鍵証明書データＣＥＲ

159

$_{SAM2}$を取り寄せる場合（図１０１中（７）など）とがある。

【０４５４】また、ＳＡＭ３０５$_2$がＳＡＭ３０５$_1$の公開鍵証明書データＣＥＲ$_{SAM1}$を取得する場合には、例えば、通信に先立ってＳＡＭ３０５$_1$からＳＡＭ３０５$_2$に公開鍵証明書データＣＥＲ$_{SAM1}$を送信する場合（図１０１中（９））と、ＳＡＭ３０５$_2$が自らＥＭＤサービスセンタ３０２から公開鍵証明書データＣＥＲ$_{SAM1}$を取り寄せる場合と、ＳＡＭ３０５$_1$が搭載されたネットワーク機器を介して公開鍵証明書データＣＥＲ$_{SAM1}$を取り寄せる場合（図１０１中（７），（８））とがある。

【０４５５】また、ＳＡＭ３０５$_4$がＳＡＭ３０５$_{13}$の公開鍵証明書データＣＥＲ$_{SAM13}$を取得する場合には、例えば、通信に先立ってＳＡＭ３０５$_{13}$からＳＡＭ３０５$_4$に公開鍵証明書データＣＥＲ$_{SAM13}$を送信する場合（図１０１中（１２））と、ＳＡＭ３０５$_4$が自らＥＭＤサービスセンタ３０２から公開鍵証明書データＣＥＲ$_{SAM13}$を取り寄せる場合（図１０１中（１０））と、ユーザホームネットワーク３０３ｂ内のネットワーク機器を介して公開鍵証明書データＣＥＲ$_{SAM13}$を取り寄せる場合とがある。

【０４５６】また、ＳＡＭ３０５$_{13}$がＳＡＭ３０５$_4$の公開鍵証明書データＣＥＲ$_{SAM4}$を取得する場合には、例えば、通信に先立ってＳＡＭ３０５$_4$からＳＡＭ３０５$_{13}$に公開鍵証明書データＣＥＲ$_{SAM4}$を送信する場合（図１０１中（１１））と、ＳＡＭ３０５$_{13}$が自らＥＭＤサービスセンタ３０２から公開鍵証明書データＣＥＲ$_{SAM4}$を取り寄せる場合（図１０１中（１３））と、ユーザホームネットワーク３０３ｂ内のネットワーク機器を介して公開鍵証明書データＣＥＲ$_{SAM4}$を取り寄せる場合とがある。

【０４５７】第２実施形態における公開鍵証明書破棄リスト（データ）の取り扱い

第２実施形態では、ＥＭＤサービスセンタ３０２において、不正行為などに用いられたコンテンツプロバイダ３０１、サービスプロバイダ３１０およびＳＡＭ３０５$_1$～３０５$_4$が他の装置と通信できないようにするために、当該不正行為に用いられた装置の公開鍵証明書データを無効にする公開鍵証明書破棄データを作成する。そして、当該公開鍵証明書破棄データＣＲＬ（Ｃｅｒｔｉｆｉｃａｔｅ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）を、コンテンツプロバイダ３０１、サービスプロバイダ３１０およびＳＡＭ３０５$_1$～３０５$_4$に送信する。なお、公開鍵証明書破棄データＣＲＬは、ＥＭＤサービスセンタ３０２の他に、例えば、コンテンツプロバイダ３０１、サービスプロバイダ３１０およびＳＡＭ３０５$_1$～３０５$_4$において生成してもよい。

【０４５８】先ず、ＥＭＤサービスセンタ３０２が、コンテンツプロバイダ３０１の公開鍵証明書データＣＥＲ

160

$_{CP}$を無効にする場合について説明する。図１０２に示すように、ＥＭＤサービスセンタ３０２は、公開鍵証明書データＣＥＲ$_{CP}$無効にすることを示す公開鍵証明書破棄データＣＲＬ$_1$をサービスプロバイダ３１０に送信する（図１０２中（１））。サービスプロバイダ３１０は、コンテンツプロバイダ３０１から入力した署名データを検証する際に、公開鍵証明書破棄データＣＲＬ$_1$を参照して公開鍵証明書データＣＥＲ$_{CP}$の有効性を判断し、有効であると判断した場合に公開鍵データＫ$_{CP,P}$を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずにコンテンツプロバイダ３０１からのデータを無効にする。なお、データを無効にするのではなく、通信を拒絶するようにしてもよい。

【０４５９】また、ＥＭＤサービスセンタ３０２は、公開鍵証明書破棄データＣＲＬ$_1$を、サービスプロバイダ３１０の流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、ユーザホームネットワーク３０３内の例えばＳＡＭ３０５$_1$に送信する（図１０２中（１），（２））。ＳＡＭ３０５$_1$は、サービスプロバイダ３１０から入力したセキュアコンテナ内に格納されたコンテンツプロバイダ３０１の署名データを検証する際に、公開鍵証明書破棄データＣＲＬ$_1$を参照して公開鍵証明書データＣＥＲ$_{CP}$の有効性を判断し、有効であると判断した場合に公開鍵データＫ$_{CP,P}$を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずに当該セキュアコンテナを無効にする。なお、ＥＭＤサービスセンタ３０２は、公開鍵証明書破棄データＣＲＬ$_1$を、ユーザホームネットワーク３０３内のネットワーク機器を介してＳＡＭ３０５$_1$に直接送信してもよい（図１０２中（３））。

【０４６０】次に、ＥＭＤサービスセンタ３０２が、サービスプロバイダ３１０の公開鍵証明書データＣＥＲ$_{SP}$を無効にする場合について説明する。図１０３に示すように、ＥＭＤサービスセンタ３０２は、公開鍵証明書データＣＥＲ$_{SP}$を無効にすることを示す公開鍵証明書破棄データＣＲＬ$_2$をコンテンツプロバイダ３０１に送信する（図１０３中（１））。コンテンツプロバイダ３０１は、サービスプロバイダ３１０から入力した署名データを検証する際に、公開鍵証明書破棄データＣＲＬ$_2$を参照して公開鍵証明書データＣＥＲ$_{SP}$の有効性を判断し、有効であると判断した場合に公開鍵データＫ$_{SP,P}$を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずにサービスプロバイダ３１０からのデータを無効にする。

【０４６１】また、ＥＭＤサービスセンタ３０２は、公開鍵証明書破棄データＣＲＬ$_2$を、サービスプロバイダ３１０の流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、ユーザホームネットワーク３０３内の例えばＳＡＭ３０５$_1$に送信する（図１０３中（２））。ＳＡＭ３０５$_1$は、サービスプロバイダ３１

０から入力したセキュアコンテナ内に格納されたサービスプロバイダ３１０の署名データを検証する際に、公開鍵証明書破棄データＣＲＬ$_2$を参照して公開鍵証明書データＣＥＲ$_{SP}$の有効性を判断し、有効であると判断した場合に公開鍵データＫ$_{SP,P}$を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずに当該セキュアコンテナを無効にする。この場合に、サービスプロバイダ３１０内において、公開鍵証明書破棄データＣＲＬ$_2$の送受信を行うモジュールは、耐タンパ性を有している必要がある。また、サービスプロバイダ３１０内において、公開鍵証明書破棄データＣＲＬ$_2$は、サービスプロバイダ３１０の関係者による改竄な困難な領域に格納される必要がある。なお、ＥＭＤサービスセンタ３０２は、公開鍵証明書破棄データＣＲＬ$_2$を、ユーザホームネットワーク３０３内のネットワーク機器を介してＳＡＭ３０５$_1$に直接送信してもよい（図１０３中（３））。

【０４６２】次に、ＥＭＤサービスセンタ３０２が、例えばＳＡＭ３０５$_2$の公開鍵証明書データＣＥＲ$_{SAM2}$を無効にする場合について説明する。図１０４に示すように、ＥＭＤサービスセンタ３０２は、公開鍵証明書データＣＥＲ$_{SAM2}$を無効にすることを示す公開鍵証明書破棄データＣＲＬ$_3$をコンテンツプロバイダ３０１に送信する（図１０４中（１））。コンテンツプロバイダ３０１は、公開鍵証明書破棄データＣＲＬ$_3$をサービスプロバイダ３１０に送信する。サービスプロバイダ３１０は、自らの流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、ユーザホームネットワーク３０３内の例えばＳＡＭ３０５$_1$に公開鍵証明書破棄データＣＲＬ$_{SAM1}$を送信する（図１０４中（１））。ＳＡＭ３０５$_1$は、ＳＡＭ３０５$_2$から入力したデータに付加されたＳＡＭ３０５$_2$の署名データを検証する際に、公開鍵証明書破棄データＣＲＬ$_3$を参照して公開鍵証明書データＣＥＲ$_{SAM2}$の有効性を判断し、有効であると判断した場合に公開鍵データＫ$_{SAM2,P}$を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずに当該データを無効にする。この場合に、サービスプロバイダ３１０内において、公開鍵証明書破棄データＣＲＬ$_3$の送受信を行うモジュールは、耐タンパ性を有している必要がある。また、サービスプロバイダ３１０内において、公開鍵証明書破棄データＣＲＬ$_3$は、サービスプロバイダ３１０の関係者による改竄な困難な領域に格納される必要がある。

【０４６３】ＥＭＤサービスセンタ３０２は、公開鍵証明書破棄データＣＲＬ$_3$をサービスプロバイダ３１０を介してＳＡＭ３０５$_1$に送信してもよい（図１０４中（１），（２））。また、ＥＭＤサービスセンタ３０２は、公開鍵証明書破棄データＣＲＬ$_3$を、ユーザホームネットワーク３０３内のネットワーク機器を介してＳＡＭ３０５$_1$に直接送信してもよい（図１０４中（３））。

【０４６４】また、ＥＭＤサービスセンタ３０２は、例えばＳＡＭ３０５$_2$の公開鍵証明書データＣＥＲ$_{SAM2}$を無効にすることを示す公開鍵証明書破棄データＣＲＬ$_3$を作成し、これを保管する。また、ユーザホームネットワーク３０３は、バス１９１に接続されているＳＡＭのＳＡＭ登録リストＳＲＬを作成し、これをＥＭＤサービスセンタ３０２に送信する（図１０５中（１））。ＥＭＤサービスセンタ３０２は、ＳＡＭ登録リストに示されるＳＡＭ３０５$_1$～３０５$_4$のうち、公開鍵証明書破棄データＣＲＬ$_3$によって無効にすることが示されているＳＡＭ（例えばＳＡＭ３０５$_2$）を特定し、ＳＡＭ登録リストＳＲＬ内の当該ＳＡＭに対応する破棄フラグを無効を示すように設定して新たなＳＡＭ登録リストＳＲＬを作成する。次に、ＥＭＤサービスセンタ３０２は、当該生成したＳＡＭ登録リストＳＲＬをＳＡＭ３０５$_1$に送信する（図１０５中（１））。ＳＡＭ３０５$_1$は、他のＳＡＭと通信を行う際に、ＳＡＭ登録リストＳＲＬの破棄フラグを参照して、署名データの検証の有無および通信を許否するか否かを決定する。

【０４６５】また、ＥＭＤサービスセンタ３０２は、公開鍵証明書破棄データＣＲＬ$_3$を作成し、これをコンテンツプロバイダ３０１に送信する（図１０５中（２））。コンテンツプロバイダ３０１は、公開鍵証明書破棄データＣＲＬ$_3$をサービスプロバイダ３１０に送信する（図１０５中（２））。次に、サービスプロバイダ３１０は、自らの流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、公開鍵証明書破棄データＣＲＬ$_3$をＳＡＭ３０５$_1$に送信する（図１０５中（２））。ＳＡＭ３０５$_1$は、自らが作成したＳＡＭ登録リストに示されるＳＡＭ３０５$_1$～３０５$_4$のうち、公開鍵証明書破棄データＣＲＬ$_3$によって無効にすることが示されているＳＡＭ（例えばＳＡＭ３０５$_2$）を特定し、ＳＡＭ登録リストＳＲＬ内の当該ＳＡＭに対応する破棄フラグを無効を示すように設定する。以後、ＳＡＭ３０５$_1$は、他のＳＡＭと通信を行う際に、当該ＳＡＭ登録リストＳＲＬの破棄フラグを参照して、署名データの検証の有無および通信を許否するか否かを決定する。

【０４６６】また、ＥＭＤサービスセンタ３０２は、公開鍵証明書破棄データＣＲＬ$_3$を作成し、これをサービスプロバイダ３１０に送信する（図１０５中（３））。次に、サービスプロバイダ３１０は、自らの流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、公開鍵証明書破棄データＣＲＬ$_3$をＳＡＭ３０５$_1$に送信する（図１０５中（３））。ＳＡＭ３０５$_1$は、自らが作成したＳＡＭ登録リストに示されるＳＡＭ３０５$_1$～３０５$_4$のうち、公開鍵証明書破棄データＣＲＬ$_3$によって無効にすることが示されているＳＡＭ（例え

ばＳＡＭ３０５$_2$）を特定し、ＳＡＭ登録リストＳＲＬ内の当該ＳＡＭに対応する破棄フラグを無効を示すように設定する。以後、ＳＡＭ３０５$_1$は、他のＳＡＭと通信を行う際に、当該ＳＡＭ登録リストＳＲＬの破棄フラグを参照して、署名データの検証の有無および通信を許否するか否かを決定する。

【０４６７】ＥＭＤサービスセンタ３０２の役割等

図１０６は、図５９に示すＥＭＤサービスセンタ（クリアリングハウス））３０２の機能を権利管理用クリアリングハウス９５０と、電子決済用クリアリングハウス９５１とに分割した場合のＥＭＤシステムの構成図である。当該ＥＭＤシステムでは、電子決済用クリアリングハウス９５１において、ユーザホームネットワーク３０３ａ，３０３ｂのＳＡＭからの利用履歴データ３０８に基づいて、決済処理（利益分配処理）を行い、コンテンツプロバイダ３０１およびサービスプロバイダ３１０の決済請求権データをそれぞれ生成し、ペイメントゲートウェイ９０を介して決済機関９１において決済を行う。

【０４６８】また、権利管理用クリアリングハウス９５０は、電子決済用クリアリングハウス９５１からの決済通知に応じたコンテンツプロバイダ３０１およびサービスプロバイダ３１０の決済レポートを作成し、それらをコンテンツプロバイダ３０１およびコンテンツプロバイダ３０１に送信する。また、コンテンツプロバイダ３０１の権利書データ１０６およびコンテンツ鍵データＫｃの登録（権威化）などを行う。なお、図１０７に示すように、権利管理用クリアリングハウス９５０と電子決済用クリアリングハウス９５１とを単体の装置内に収納すると、図５９に示すＥＭＤサービスセンタ３０２となる。

【０４６９】また、本発明は、例えば、図１０８に示すように、ＥＭＤサービスセンタ３０２に、権利管理用クリアリングハウス９６０の機能を設け、権利管理用クリアリングハウス９６０において、権利書データ１０６の登録などを行うと共に、ＳＡＭからの利用履歴データ３０８に基づいてサービスプロバイダ３１０の決済請求権データを作成し、これをサービスプロバイダ３１０に送信してもよい。この場合には、サービスプロバイダ３１０は、自らの課金システムを電子決済用クリアリングハウス９６１として利用し、権利管理用クリアリングハウス９６０からの決済請求権データに基づいて決済を行う。

【０４７０】また、本発明は、例えば、図１０９に示すように、ＥＭＤサービスセンタ３０２に、権利管理用クリアリングハウス９７０の機能を設け、権利管理用クリアリングハウス９７０において、権利書データ１０６の登録などを行うと共に、ＳＡＭからの利用履歴データ３０８に基づいてコンテンツプロバイダ３０１の決済請求権データを作成し、これをコンテンツプロバイダ３０１に送信してもよい。この場合には、コンテンツプロバイダ３０１は、自らの課金システムを電子決済用クリアリングハウス９６１として利用し、権利管理用クリアリングハウス９７０からの決済請求権データに基づいて決済を行う。

【０４７１】また、本発明は、例えば、図１１０に示すように、コンテンツプロバイダ３０１内に、前述した権利管理用クリアリングハウス９７０および電子決済用クリアリングハウス９７１の機能を備えるようにしてもよい。この場合には、コンテンツプロバイダ３０１は、自らの課金システムを電子決済用クリアリングハウス９６１として利用し、権利管理用クリアリングハウス９７０において生成した決済請求権データに基づいて、決済機関９１に対して自ら決済を行う。

【０４７２】第２実施形態の第８変形例

上述した第２実施形態では、図５９に示すＥＭＤシステム３００において、コンテンツプロバイダ３０１からサービスプロバイダ３１０に図５に示すフォーマットのセキュアコンテナ１０４を提供し、サービスプロバイダ３１０からユーザホームネットワーク３０３に図６５に示すフォーマットのセキュアコンテナ３０４を配給する場合を例示した。すなわち、上述した第２実施形態では、図５および図６５に示すように、セキュアコンテナ１０４およびセキュアコンテナ３０４内に、それぞれ単数のコンテンツファイルＣＦと、当該コンテンツファイルＣＦに対応する単数のキーファイルＫＦを格納した場合を例示した。本発明では、セキュアコンテナ１０４およびセキュアコンテナ３０４内に、それぞれ複数のコンテンツファイルＣＦと、当該複数のコンテンツファイルＣＦにそれぞれ対応する複数のキーファイルＫＦとを格納してもよい。

【０４７３】図１１１は、本変形例において、図５９に示すコンテンツプロバイダ３０１からサービスプロバイダ３１０に提供されるセキュアコンテナ１０４ａのフォーマットを説明するための図である。図１１１に示すように、セキュアコンテナ１０４ａには、コンテンツファイルＣＦ$_1$，ＣＦ$_2$，ＣＦ$_3$、キーファイルＫＦ$_1$，ＫＦ$_2$，ＫＦ$_3$、公開鍵証明書データＣＥＲ$_{CP}$、署名データＳＩＧ$_{200,CP}$，ＳＩＧ$_{201,CP}$，ＳＩＧ$_{202,CP}$，ＳＩＧ$_{203,CP}$，ＳＩＧ$_{204,CP}$，ＳＩＧ$_{205,CP}$，ＳＩＧ$_{1,ESC}$が格納されている。ここで、署名データＳＩＧ$_{200,CP}$，ＳＩＧ$_{201,CP}$，ＳＩＧ$_{202,CP}$，ＳＩＧ$_{203,CP}$，ＳＩＧ$_{204,CP}$，ＳＩＧ$_{205,CP}$は、コンテンツプロバイダ３０１において、それぞれコンテンツファイルＣＦ$_1$，ＣＦ$_2$，ＣＦ$_3$，キーファイルＫＦ$_1$，ＫＦ$_2$，ＫＦ$_3$に対してハッシュ値をとり、コンテンツプロバイダ３０１の秘密鍵データＫ$_{cp,s}$を用いて生成される。

【０４７４】コンテンツファイルＣＦ$_1$には、ヘッダ、

メタデータＭｅｔａ$_1$、コンテンツデータＣ$_1$，Ａ／Ｖ伸長用ソフトウェアＳｏｆｔ$_1$および電子透かし情報モジュールＷＭ$_1$が格納されている。ここで、コンテンツデータＣ$_1$およびＡ／Ｖ伸長用ソフトウェアＳｏｆｔ$_1$は、コンテンツ鍵データＫｃ$_1$を用いて暗号化されており、メタデータＭｅｔａ$_1$および電子透かし情報モジュールＷＭ$_1$は必要に応じてコンテンツ鍵データＫｃ$_1$を用いて暗号化されている。また、コンテンツデータＣ$_1$は、例えば、ＡＴＲＡＣ３方式で圧縮されている。Ａ／Ｖ伸長用ソフトウェアＳｏｆｔ$_1$は、ＡＴＲＡＣ３方式の伸長用のソフトウェアである。また、コンテンツファイルＣＦ$_1$のヘッダには、例えば、図１１２に示すようにキーファイルＫＦ$_1$およびコンテンツファイルＣＦ$_2$にリンクすることを示すディレクトリ構造データＤＳＤ$_1$が含まれている。

【０４７５】コンテンツファイルＣＦ$_2$には、ヘッダ、メタデータＭｅｔａ$_2$、コンテンツデータＣ$_2$、Ａ／Ｖ伸長用ソフトウェアＳｏｆｔ$_2$および電子透かし情報モジュールＷＭ$_2$が格納されている。ここで、コンテンツデータＣ$_2$およびＡ／Ｖ伸長用ソフトウェアＳｏｆｔ$_2$は、コンテンツ鍵データＫｃ$_2$を用いて暗号化されており、メタデータＭｅｔａ$_2$および電子透かし情報モジュールＷＭ$_2$は必要に応じてコンテンツ鍵データＫｃ$_2$を用いて暗号化されている。また、コンテンツデータＣ$_2$は、例えば、ＭＰＥＧ２方式で圧縮されている。Ａ／Ｖ伸長用ソフトウェアＳｏｆｔ$_2$は、ＭＰＥＧ２方式の伸長用のソフトウェアである。また、コンテンツファイルＣＦ$_2$のヘッダには、例えば、図１１２に示すように、キーファイルＫＦ$_2$およびコンテンツファイルＣＦ$_3$にリンクすることを示すディレクトリ構造データＤＳＤ$_2$が含まれている。

【０４７６】コンテンツファイルＣＦ$_3$には、ヘッダ、メタデータＭｅｔａ$_3$、コンテンツデータＣ$_3$、Ａ／Ｖ伸長用ソフトウェアＳｏｆｔ$_3$および電子透かし情報モジュールＷＭ$_3$が格納されている。ここで、コンテンツデータＣ$_3$およびＡ／Ｖ伸長用ソフトウェアＳｏｆｔ$_3$は、コンテンツ鍵データＫｃ$_3$を用いて暗号化されており、メタデータＭｅｔａ$_3$および電子透かし情報モジュールＷＭ$_3$は必要に応じてコンテンツ鍵データＫＣ$_3$を用いて暗号化されている。また、コンテンツデータＣ$_3$は、例えば、ＪＰＥＧ方式で圧縮されている。Ａ／Ｖ伸長用ソフトウェアＳｏｆｔ$_3$は、ＪＰＥＧ方式の伸長用のソフトウェアである。また、コンテンツファイルＣＦ$_3$のヘッダには、例えば、図１１２に示すように、キーファイルＫＦ$_3$にリンクすることを示すディレクトリ構造データＤＳＤ$_3$が含まれている。

【０４７７】キーファイルＫＦ$_1$には、ヘッダと、配信鍵データＫＤ$_1$～ＫＤ$_3$を用いて暗号化されたコンテンツ鍵データＫｃ$_1$、権利書データ１０６$_1$およびＳＡＭプログラム・ダウンロード・コンテナＳＤＣ$_1$と、署名データＳＩＧ$_{220,ESC}$とが格納されている。

【０４７８】キーファイルＫＦ$_2$には、ヘッダと、配信鍵データＫＤ$_1$～ＫＤ$_3$を用いて暗号化されたコンテンツ鍵データＫｃ$_2$、権利書データ１０６$_2$およびＳＡＭプログラム・ダウンロード・コンテナＳＤＣ$_2$と、署名データＳＩＧ$_{221,ESC}$とが格納されている。

【０４７９】キーファイルＫＦ$_3$には、ヘッダと、配信鍵データＫＤ$_1$～ＫＤ$_3$を用いて暗号化されたコンテンツ鍵データＫｃ$_3$、権利書データ１０６$_3$およびＳＡＭプログラム・ダウンロード・コンテナＳＤＣ$_3$と、署名データＳＩＧ$_{222,ESC}$とが格納されている。

【０４８０】サービスプロバイダ３１０は、図１１２に示すセキュアコンテナ１０４ａの配給を受けると、ＥＭＤサービスセンタ３０２の公開鍵データＫ$_{ESC,P}$を用いて公開鍵証明書データＣＥＲ$_{CP}$の正当性を確認した後に、当該公開鍵証明書データＣＥＲ$_{CP}$に格納された公開鍵データＫ$_{CP,P}$を用いて、署名データＳＩＧ$_{200,CP}$，ＳＩＧ$_{201,CP}$，ＳＩＧ$_{202,CP}$，ＳＩＧ$_{203,CP}$，ＳＩＧ$_{204,CP}$，ＳＩＧ$_{205,CP}$の正当性、すなわちコンテンツファイルＣＦ$_1$，ＣＦ$_2$，ＣＦ$_3$の作成者および送信者の正当性と、キーファイルＫＦ$_1$，ＫＦ$_2$，ＫＦ$_3$の送信者の正当性を確認する。また、コンテンツプロバイダ３０１は、公開鍵データＫ$_{ESC,P}$を用いて、署名データＳＩＧ$_{220,ESC}$，ＳＩＧ$_{221,ESC}$，ＳＩＧ$_{222,ESC}$の正当性、キーファイルＫＦ$_1$，ＫＦ$_2$，ＫＦ$_3$の作成者の正当性を確認する。

【０４８１】そして、サービスプロバイダ３１０は、コンテンツファイルＣＦ$_1$，ＣＦ$_2$，ＣＦ$_3$の販売価格を示すプライスタグデータ３１２$_1$，３１２$_2$，３１２$_3$を作成する。また、サービスプロバイダ３１０は、秘密鍵データＫ$_{SP,S}$を用いて、プライスタグデータ３１２$_1$，３１２$_2$，３１２$_3$の署名データＳＩＧ$_{220,SP}$，ＳＩＧ$_{221,SP}$，ＳＩＧ$_{222,SP}$を作成する。また、サービスプロバイダ３１０は、秘密鍵データＫ$_{SP,S}$を用いて、コンテンツファイルＣＦ$_1$，ＣＦ$_2$，ＣＦ$_3$，ＫＦ$_1$，ＫＦ$_2$，ＫＦ$_3$の署名データＳＩＧ$_{210,SP}$，ＳＩＧ$_{211,SP}$，ＳＩＧ$_{212,SP}$，ＳＩＧ$_{213,SP}$，ＳＩＧ$_{214,SP}$，ＳＩＧ$_{215,SP}$を作成する。

【０４８２】次に、サービスプロバイダ３１０は、図１１４に示すセキュアコンテナ３０４ａを作成する。

【０４８３】サービスプロバイダ３１０は、図１１４に示すセキュアコンテナ３０４ａをユーザホームネットワーク３０３に配給する。ユーザホームネットワーク３０３では、ＳＡＭ３０５$_1$～３０５$_4$において、セキュアコンテナ３０４ａに格納された全ての署名データの正当性を確認した後に、コンテンツデータＣ$_1$，Ｃ$_2$，Ｃ$_3$

についての権利処理を、ディレクトリ構造データＤＳＤ１～ＤＳＤ３に示されるリンク状態に応じて、それぞれキーファイルＫＦ１，ＫＦ２，ＫＦ３に基づいて行う。

【０４８４】また、上述した第８変形例では、セキュアコンテナ３０４において、単数のサービスプロバイダ３１０から提供を受けた複数のコンテンツファイルＣＦ１０１，ＣＦ１０２，ＣＦ１０３を単数のセキュアコンテナ３０４ａに格納してユーザホームネットワーク３０３に配給する場合を例示したが、図９８に示すように、複数のコンテンツプロバイダ３０１ａ，３０１ｂから提供を受けた複数のコンテンツファイルＣＦを、単数のセキュアコンテナに格納してユーザホームネットワーク３０３に配給してもよい。

【０４８５】また、セキュアコンテナ１０４，３０４内には、例えば、図１１３に示すように、ＡＴＲＡＣ３で圧縮された楽曲（音声）データを格納したコンテンツファイルＣＦ１，ＭＰＥＧ２で圧縮されたビデオクリップデータを格納したコンテンツファイルＣＦ２，ＪＰＥＧで圧縮されたジャケット（静止画）データを格納したコンテンツファイルＣＦ３、テキスト形式の歌詞データを格納したコンテンツファイルＣＦ４並びにテキスト形式のライナーノーツデータを格納したコンテンツファイルＣＦ５と、それぞれに対応したキーファイルＫＦ１，ＫＦ２，ＫＦ３，ＫＦ４，ＫＦ５とを格納してもよい。この場合にも、同様に、コンテンツファイルＣＦ１～ＣＦ５のディレクトリ構造データによって、コンテンツファイルＣＦ１～ＣＦ５相互間のリンクと、コンテンツファイルＣＦ１～ＣＦ５とキーファイルＫＦ１～ＫＦ５との間のそれぞれのリンクとが確立される。

【０４８６】なお、本実施形態におけるセキュアコンテナ内に複数のコンテンツデータを格納する場合（コンポジット型の場合）のデータフォーマットの概念は、例えば、図１１５あるいは図１１６に示される。

【０４８７】なお、図１１１に示すフォーマットは、前述した第１実施形態において、図１に示すコンテンツプロバイダ１０１からユーザホームネットワーク１０３にセキュアコンテナ１０４を送信する場合にも同様に適用できる。

【０４８８】第２実施形態の第９変形例

上述した実施形態では、コンテンツファイルＣＦおよびキーファイルＫＦをディレクトリ構造でセキュアコンテナ１０４，３０４に格納してコンテンツプロバイダ３０１からサービスプロバイダ３１０、並びにサービスプロバイダ３１０からＳＡＭ３０５１～３０５４に送信する場合を例示したが、コンテンツファイルＣＦおよびキーファイルＫＦを、別々にコンテンツプロバイダ３０１からサービスプロバイダ３１０、並びにサービスプロバイダ３１０からＳＡＭ３０５１～３０５４に送信してもよい。これには、例えば、以下に示す第１の手法と第２の手法とがある。第１の手法では、図１１７に示すよう

に、コンテンツプロバイダ３０１からサービスプロバイダ３１０、並びにサービスプロバイダ３１０からＳＡＭ３０５１～３０５４に、コンテンツファイルＣＦおよびキーファイルＫＦを別々に送信する。また、第２の手法では、図１１８に示すように、コンテンツプロバイダ３０１からサービスプロバイダ３１０、並びにサービスプロバイダ３１０からＳＡＭ３０５１～３０５４にコンテンツファイルＣＦを送信し、ＥＭＤサービスセンタ３０２からＳＡＭ３０５１～３０５４にキーファイルＫＦを送信する。当該キーファイルＫＦの送信は、例えば、ＳＡＭ３０５１～３０５４のユーザが、コンテンツデータＣの購入形態を決定しようとするときに、ＥＭＤサービスセンタ３０２からＳＡＭ３０５１～３０５４に送信される。上述した第１の手法および第２の手法を採用する場合には、例えば、関連するコンテンツファイルＣＦ相互間と、コンテンツファイルＣＦとそれに対応するキーファイルＫＦとの間を、コンテンツファイルＣＦおよびキーファイルＫＦの少なくとも一方のヘッダに格納されたハイパーリンクデータＨＬを用いてリンク関係を確立する。ＳＡＭ１０５１～１０５４では、当該リンク関係に基づいて、コンテンツデータＣの権利処理および利用を行う。

【０４８９】また、上述した第２実施形態では、コンテンツデータＣと、コンテンツ鍵データＫｃおよび権利書データ１０６などの鍵データとをそれぞれファイル形式にして、コンテンツプロバイダ３０１からサービスプロバイダ３１０、並びにサービスプロバイダ３１０からＳＡＭ３０５１～３０５４に送信する場合を例示したが、これらは、相互間でのリンク関係が確立できれば、必ずしもファイル形式にする必要はない。例えば、図１１９に示すように、コンテンツデータＣ、メタデータＭｅｔａ、Ａ／Ｖ伸長用ソフトウェアＳｏｆｔ、電子透かし情報モジュールＷＭ、キーファイルＫＦ、プライスタグデータ３１２および、公開鍵証明書データＣＥＲｃｐ，ＣＥＲｓｐを別々に、コンテンツプロバイダ３０１およびＥＭＤサービスセンタ３０２からＳＡＭ３０５１～３０５４に送信してもよい。この場合には、図１１９に示すように、コンテンツデータＣ、メタデータＭｅｔａ、Ａ／Ｖ伸長用ソフトウェアＳｏｆｔ、電子透かし情報モジュールＷＭ、キーファイルＫＦ、プライスタグデータ３１２、公開鍵証明書データＣＥＲｃｐ，ＣＥＲｓｐが、ハイパーリンクデータＨＬによってリンクされる。ここで、ハイパーリンクデータＨＬは、例えば、配信用鍵データＫＤ１～ＫＤ６で暗号化されて送信される。

【０４９０】なお、本変形例において、コンテンツファイルＣＦおよびキーファイルＫＦのフォーマットは、例えば、図５（Ａ），（Ｂ）に示すものが採用される。また、この場合に、コンテンツファイルＣＦおよびキーファイルＫＦと共に、それらの署名データＳＩ

$G_{6,cp}$，$SIG_{7,cp}$を送信することが好ましい。

【０４９１】第２実施形態の第１０変形例

上述した実施形態では、セキュアコンテナ１０４内において、コンテンツファイルＣＦおよびキーファイルＫＦを別々に設けた場合を例示したが、例えば、図１２０に示すように、セキュアコンテナ１０４，３０４内において、コンテンツファイルＣＦ内にキーファイルＫＦを格納するようにしてもよい。この場合に、キーファイルＫＦを格納したコンテンツファイルＣＦに対して、コンテンツプロバイダ３０１の秘密鍵データ$Kc_{P,s}$による署名データ、並びにサービスプロバイダ３１０の秘密鍵データ$Ks_{P,s}$による署名データが付される。

第２実施形態の第１１変形例

上述した実施形態では、コンテンツデータＣをコンテンツファイルＣＦに格納し、コンテンツ鍵データＫｃおよび権利書データ１０６をキーファイルＫＦ内に格納してコンテンツプロバイダ３０１からサービスプロバイダ３１０、並びにサービスプロバイダ３１０から$SAM305_1$などに送信する場合を例示したが、コンテンツデータＣ、コンテンツ鍵データＫｃおよび権利書データ１０６の少なくとも一つをファイル形式を採用せずにコンテンツプロバイダ３０１からサービスプロバイダ３１０、並びにサービスプロバイダ３１０から$SAM305_1$などに、通信プロトコルに依存しない形式で送信してもよい。

【０４９２】例えば、図１２１に示すように、コンテンツプロバイダ３０１において、コンテンツ鍵データＫｃで暗号化されたコンテンツデータＣと、暗号化されたコンテンツ鍵データＫｃおよび暗号化された権利書データ１０６などを含むキーファイルＫＦとを格納したセキュアコンテナ１０４ｓを作成し、セキュアコンテナ１０４ｓをサービスプロバイダ３１０に通信プロトコルに依存しない形式で送信する。そして、サービスプロバイダ３１０において、セキュアコンテナ１０４ｓに格納されたコンテンツデータＣおよびキーファイルＫＦにプライスタグデータ３１２を加えてセキュアコンテナ３０４ｓを作成し、セキュアコンテナ３０４ｓを$SAM305_1$などに通信プロトコルに依存しない形式で送信してもよい。

【０５９３】また、図１２２に示すように、コンテンツプロバイダ３０１からサービスプロバイダ３１０に、コンテンツ鍵データＫｃで暗号化されたコンテンツデータＣと、暗号化されたコンテンツ鍵データＫｃおよび暗号化された権利書データ１０６などを含むキーファイルＫＦとを通信プロトコルに依存しない形式で個別に送信する。そして、サービスプロバイダ３１０から$SAM305_1$などに、コンテンツデータＣ、キーファイルＫＦおよびプライスタグデータ３１２を通信プロトコルに依存しない形式で個別に送信する。すなわち、コンテンツデータＣをファイル形式にしないで、キーファイルＫＦと同一経路で送信する。

【０４９４】また、図１２３に示すように、コンテンツプロバイダ３０１からサービスプロバイダ３１０に、コンテンツ鍵データＫｃで暗号化されたコンテンツデータＣを通信プロトコルに依存しない形式で送信し、サービスプロバイダ３１０から$SAM305_1$などにコンテンツデータＣおよびプライスタグデータ３１２を通信プロトコルに依存しない形式で送信する。また、暗号化されたコンテンツ鍵データＫｃおよび暗号化された権利書データ１０６などを含むキーファイルＫＦをＥＭＤサービスセンタ３０２から$SAM305_1$などに送信してもよい。すなわち、コンテンツデータＣをファイル形式にしないで、キーファイルＫＦと別経路で送信する。

【０４９５】また、図１２４に示すように、コンテンツプロバイダ３０１からサービスプロバイダ３１０に、コンテンツ鍵データＫｃで暗号化されたコンテンツデータＣと、コンテンツ鍵データＫｃおよび権利書データ１０６とを、通信プロトコルに依存しない形式で送信する。また、サービスプロバイダ３１０から$SAM305_1$などに、コンテンツデータＣ、コンテンツ鍵データＫｃおよび権利書データ１０６、並びにプライスタグデータ３１２を送信する。すなわち、コンテンツデータＣ、コンテンツ鍵データＫｃ、権利書データ１０６およびプライスタグデータ３１２をファイル形式にしないで、同一経路で送信する。

【０４９６】また、図１２５に示すように、コンテンツプロバイダ３０１からサービスプロバイダ３１０に、コンテンツ鍵データＫｃで暗号化されたコンテンツデータＣを、通信プロトコルに依存しない形式で送信する。そして、サービスプロバイダ３１０から$SAM305_1$などに、コンテンツデータＣおよびプライスタグデータ３１２を、通信プロトコルに依存しない形式で送信する。また、ＥＭＤサービスセンタ３０２から$SAM305_1$などにコンテンツ鍵データＫｃおよび権利書データ１０６を送信する。。すなわち、コンテンツデータＣと、コンテンツ鍵データＫｃおよび権利書データ１０６とをファイル形式にしないで、別経路で送信する。

【０４９７】第２実施形態の第１２変形例

前述した図５９に示すＥＭＤシステム３００では、例えば、図１２６に示すように、ユーザホームネットワーク３０３がサービスプロバイダ３１０から受信したセキュアコンテナ３０４に応じたセキュアコンテナ３０４Ａを、ユーザホームネットワーク３０３ａのＳＡＭからの要求Ｓ３０３ａに応じて、ユーザホームネットワーク３０３ａに配給してもよい。この場合には、ユーザホームネットワーク３０３のＳＡＭが、前述した第２実施形態で説明したサービスプロバイダ３１０と同様の役割を果たすと考えることができる。この場合に、ユーザホームネットワーク３０３ａのＳＡＭは、独自にプライスタグ

データ３１２を新たに設定できる。そして、ユーザホームネットワーク３０３ａのＳＡＭにおいてコンテンツデータＣの購入形態が決定され、それに応じた利用履歴データ３０４ａなどがユーザホームネットワーク３０３ａのＳＡＭからＥＭＤサービスセンタ３０２に送信される。ＥＭＤサービスセンタ３０２では、利用履歴データ３０４ａに基づいて、コンテンツプロバイダ３０１、サービスプロバイダ３１０、ユーザホームネットワーク３０３のユーザに、ユーザホームネットワーク３０３ａのユーザが支払った金銭を分配するための決済処理を行う。

【０４９８】なお、本実施形態におけるセキュアコンテナのファイル包括大小関係は、図１２７に示すように表現できる。

【０４９９】第３実施形態

図１２８は本発明の第３実施形態のＥＭＤシステムを説明するための図、図１２９は図１２８に示すＥＭＤサービスセンタの機能ブロック図である。図１２９において、前述した第１実施形態および第２実施形態で用いた符号と同じ符号を付した構成要素は、これらの実施形態で説明した同一符号の構成要素と同じである。

【０５００】本実施形態のＥＭＤシステムでは、コンテンツプロバイダ３０１はＥＭＤサービスセンタ３０２にマスタソース（コンテンツデータ）Ｓ１１１などを送り、ＥＭＤサービスセンタ３０２において例えば図５（Ａ）に示すコンテンツファイルＣＦを作成する。また、コンテンツプロバイダ３０１はＥＭＤサービスセンタ３０２に、コンテンツデータＳ１１１のコンテンツＩＤ、コンテンツ鍵データＫｃ、電子透かし管理情報（コンテンツデータに埋め込む電子透かし情報の内容）、コンテンツプロバイダ３０１の識別子ＣＰ＿ＩＤ、コンテンツデータを提供するサービスプロバイダ３１０の識別子ＳＰ＿ＩＤ、コンテンツデータの卸売価格ＳＲＰを送り、ＥＭＤサービスセンタ３０２において図５（Ｂ）に示すキーファイルＫＦを作成する。また、ＥＭＤサービスセンタ３０２は、作成したコンテンツファイルＣＦをＣＦデータベース８０２ａに格納し、個々のコンテンツファイルＣＦにグローバルユニークなコンテンツＩＤを付して、これらを一元的に管理する。また、ＥＭＤサービスセンタ３０２は、キーファイルＫＦをＫＦデータベース１５３ａに格納し、これについてもコンテンツＩＤを用いて一元的に管理する。

【０５０１】ＥＭＤサービスセンタ３０２における処理を図１２９を参照して説明する。ＥＭＤサービスセンタ３０２は、コンテンツプロバイダ３０１から受け取ったマスタソースＳ１１１をコンテンツマスタソースデータベース８０１に格納する。次に、電子透かし情報付加部１１２において、コンテンツプロバイダ３０１から受け取った電子透かし管理情報が示す電子透かし情報を、コンテンツマスタソースデータベース８０１から読み出したマスタソースＳ１１１に埋め込んでコンテンツデータＳ１１２を生成する。次に、圧縮部１１３において、コンテンツデータＳ１１２を圧縮してコンテンツデータＳ１１３を生成する。コンテンツデータＳ１１２は、伸長部１１６において伸長された後に、聴感検査部１２３において聴覚検査が行われ、必要であれば、電子透かし情報付加部１１２において電子透かし情報が再び埋め込まれる。次に、暗号化部１１４において、コンテンツデータＳ１１３がコンテンツ鍵データＫｃを用いて暗号化されてコンテンツデータＳ１１４が生成される。次に、ＣＦ作成部８０２において、コンテンツデータＳ１１４などを格納した図５（Ａ）に示すコンテンツファイルＣＦが作成され、コンテンツファイルＣＦがＣＦデータベース８０２ａに格納される。

【０５０２】また、ＥＭＤサービスセンタ３０２では、ＫＦ作成部１５３において、図５（Ｂ）に示すキーファイルＫＦを作成し、キーファイルＫＦをＫＦデータベース１５３ａに格納する。

【０５０３】次に、セキュアコンテナ作成部８０４において、ＣＦデータベース８０２ａから読み出したコンテンツファイルＣＦと、ＫＦデータベース１５３ａから読み出したキーファイルＫＦとを格納したセキュアコンテナ８０６が作成され、セキュアコンテナ８０６がセキュアコンテナデータベース８０５に格納される。その後、セキュアコンテナデータベース８０５が、サービスプロバイダ３１０によってアクセスされて、セキュアコンテナ８０６がサービスプロバイダ３１０に供給される。

【０５０４】次に、サービスプロバイダ３１０は、セキュアコンテナ８０６に格納されたコンテンツファイルＣＦおよびキーファイルＫＦと、コンテンツデータの販売価格を示すプライスタグデータ３１２とを格納したセキュアコンテナ８０７を作成する。そして、サービスプロバイダ３１０は、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいはＲＯＭ型などの記録媒体に記録してセキュアコンテナ８０７をユーザホームネットワーク３０３に配給する。

【０５０５】ユーザホームネットワーク３０３では、オインラインの場合にはＣＡモジュール３１１を介してセキュアコンテナ８０７がＳＡＭ3051などに提供され、ＳＡＭ3051などにおいて、キーファイルＫＦに格納されたコンテンツ鍵データＫｃおよび権利書データ１０６などが配信用鍵データKD_1～KD_3などを用いて復号され、復号された権利書データ１０６に基づいて、コンテンツファイルＣＦに格納されたコンテンツデータの購入形態などの取り扱いが決定される。また、ＳＡＭ3051などにおいて、コンテンツデータの購入履歴などを示す利用履歴データ３０８が生成され、利用履歴データ３０８がＥＭＤサービスセンタ３０２に送信される。また、ユーザホームネットワーク３０３のＳＡＭ3052から、ユーザホームネットワーク３０３ａのＳ

ＡＭ３０５₁₂にセキュアコンテナ８０７が配給された場合には、ＳＡＭ３０５₁₂においてＳＡＭ３０５₂と同様の処理が行われ、ＳＡＭ３０５₁₂からＥＭＤサービスセンタ３０２に利用履歴データ３０８が送信される。

【０５０６】なお、ユーザホームネットワーク３０３，３０３ａにおけるセキュアコンテナ８０７に対しての処理は、前述した第１実施形態および第２実施形態におけるユーザホームネットワーク１０３，３０３における処理と同じである。また、図１２８に示す例では、ＥＭＤサービスセンタ３０２からサービスプロバイダ３１０、並びにサービスプロバイダ３１０からユーザホームネットワーク３０３に、コンテンツファイルＣＦおよびキーファイルＫＦを格納したセキュアコンテナを送信する場合（イン・バンドの場合）を例示したが、コンテンツファイルＣＦおよびキーファイルＫＦを同一経路で別々に送信してもよい（アウト・オブ・バンドの場合）。また、図１３０に示すように、ＥＭＤサービスセンタ３０２において作成したコンテンツファイルＣＦをサービスプロバイダ３１０に供給し、サービスプロバイダ３１０がコンテンツファイルＣＦをユーザホームネットワーク３０３に供給すると共に、ＥＭＤサービスセンタ３０２において作成したキーファイルＫＦをＥＭＤサービスセンタ３０２からユーザホームネットワーク３０３，３０３ａのＳＡＭ３０５₂，ＳＡＭ３０５₁₂に供給してもよい。

【０５０７】第４実施形態

図１３１は本発明の第４実施形態のＥＭＤシステムを説明するための図である。

【０５０８】本実施形態のＥＭＤシステムでは、コンテンツプロバイダ３０１は例えば図５（Ａ）に示すコンテンツファイルＣＦを作成し、これをＥＭＤサービスセンタ３０２に送る。また、コンテンツプロバイダ３０１はＥＭＤサービスセンタ３０２に、コンテンツデータのコンテンツＩＤ、コンテンツ鍵データＫｃ、電子透かし管理情報（コンテンツデータに埋め込む電子透かし情報の内容、並びに埋め込み位置情報）、コンテンツプロバイダ３０１の識別子ＣＰ＿ＩＤ、コンテンツデータを提供するサービスプロバイダ３１０の識別子ＳＰ＿ＩＤ、コンテンツデータの卸売価格ＳＲＰを送り、ＥＭＤサービスセンタ３０２において図５（Ｂ）に示すキーファイルＫＦを作成する。また、ＥＭＤサービスセンタ３０２は、コンテンツファイルＣＦをＣＦデータベース８０２ａに格納し、個々のコンテンツファイルＣＦにグローバルユニークなコンテンツＩＤを付して、これらを一元的に管理する。また、ＥＭＤサービスセンタ３０２は、作成したキーファイルＫＦをＫＦデータベース１５３ａに格納し、これについてもコンテンツＩＤを用いて一元的に管理する。

【０５０９】また、ＥＭＤサービスセンタ３０２では、ＣＦデータベース８０２ａから読み出したコンテンツファイルＣＦと、ＫＦデータベース１５３ａから読み出したキーファイルＫＦとを格納したセキュアコンテナ８０６が作成され、セキュアコンテナ８０６がセキュアコンテナデータベースに格納される。その後、セキュアコンテナデータベースが、サービスプロバイダ３１０によってアクセスされて、セキュアコンテナ８０６がサービスプロバイダ３１０に供給される。

【０５１０】次に、サービスプロバイダ３１０は、セキュアコンテナ８０６に格納されたコンテンツファイルＣＦおよびキーファイルＫＦと、コンテンツデータの販売価格を示すプライスタグデータ３１２とを格納したセキュアコンテナ８０７を作成する。そして、サービスプロバイダ３１０は、所定の通信プロトコルを用いて当該通信プロトコルに依存しない形式で、あるいはＲＯＭ型などの記録媒体に記録してセキュアコンテナ８０７をユーザホームネットワーク３０３に配給する。

【０５１１】ユーザホームネットワーク３０３では、オインラインの場合にはＣＡモジュール３１１を介してセキュアコンテナ８０７がＳＡＭ３０５₁などに提供され、ＳＡＭ３０５₁などにおいて、キーファイルＫＦに格納されたコンテンツ鍵データＫｃおよび権利書データ１０６などが配信用鍵データＫＤ₁～ＫＤ₃などを用いて復号され、復号された権利書データ１０６に基づいて、コンテンツファイルＣＦに格納されたコンテンツデータの購入形態などの取り扱いが決定される。また、ＳＡＭ３０５₁などにおいて、コンテンツデータの購入履歴などを示す利用履歴データ３０８が生成され、利用履歴データ３０８がＥＭＤサービスセンタ３０２に送信される。また、ユーザホームネットワーク３０３のＳＡＭ３０５₂から、ユーザホームネットワーク３０３ａのＳＡＭ３０５₁₂にセキュアコンテナ８０７が配給された場合には、ＳＡＭ３０５₁₂においてＳＡＭ３０５₂と同様の処理が行われ、ＳＡＭ３０５₁₂からＥＭＤサービスセンタ３０２に利用履歴データ３０８が送信される。

【０５１２】なお、ユーザホームネットワーク３０３，３０３ａにおけるセキュアコンテナ８０７に対しての処理は、前述した第１実施形態および第２実施形態におけるユーザホームネットワーク１０３，３０３における処理と同じである。また、図１３１に示す例では、ＥＭＤサービスセンタ３０２からサービスプロバイダ３１０、並びにサービスプロバイダ３１０からユーザホームネットワーク３０３に、コンテンツファイルＣＦおよびキーファイルＫＦを格納したセキュアコンテナを送信する場合（イン・バンドの場合）を例示したが、コンテンツファイルＣＦおよびキーファイルＫＦを同一経路で別々に送信してもよい（アウト・オブ・バンドの場合）。また、図１３２に示すように、コンテンツファイルＣＦをＥＭＤサービスセンタ３０２からサービスプロバイダ３

175

１０に供給し、サービスプロバイダ３１０がコンテンツファイルＣＦをユーザホームネットワーク３０３に供給すると共に、ＥＭＤサービスセンタ３０２において作成したキーファイルＫＦをＥＭＤサービスセンタ３０２からユーザホームネットワーク３０３，３０３ａのＳＡＭ３０５$_{12}$，ＳＡＭ３０５$_{12}$に供給してもよい。

【０５１３】第５実施形態

図１３３は本発明の第５実施形態のＥＭＤシステムを説明するための図である。

【０５１４】本実施形態のＥＭＤシステムでは、コンテンツプロバイダ３０１は例えば図５（Ａ）に示すコンテンツファイルＣＦを作成する。また、コンテンツプロバイダ３０１はＥＭＤサービスセンタ３０２に、コンテンツデータのコンテンツＩＤ、コンテンツ鍵データＫｃ、電子透かし管理情報（コンテンツデータに埋め込む電子透かし情報の内容、並びに埋め込み位置情報）、コンテンツプロバイダ３０１の識別子ＣＰ＿ＩＤ、コンテンツデータを提供するサービスプロバイダ３１０の識別子ＳＰ＿ＩＤ、コンテンツデータの卸売価格ＳＲＰを送り、ＥＭＤサービスセンタ３０２において図５（Ｂ）に示すキーファイルＫＦを作成する。ＥＭＤサービスセンタ３０２は、作成したキーファイルＫＦをコンテンツプロバイダ３０１に送る。また、ＥＭＤサービスセンタ３０２は、ＫＦデータベース１５３ａにキーファイルＫＦを格納し、個々のコンテンツデータに割り当てられたコンテンツＩＤを用いてキーファイルＫＦを一元的に管理する。このとき、コンテンツＩＤは、例えば、ＥＭＤサービスセンタ３０２によって作成され、複数のコンテンツプロバイダ３０１が提供するコンテンツデータの全てを対象としてグローバルユニークに決定される。

【０５１５】次に、コンテンツプロバイダ３０１において、作成したコンテンツファイルＣＦと、ＥＭＤサービスセンタ３０２から受けたキーファイルＫＦとを格納したセキュアコンテナ８２１が作成され、セキュアコンテナ８２１が共通データベース８２０に格納される。共通データベース８２０において、複数のコンテンツプロバイダ３０１が提供したセキュアコンテナ８２１が、コンテンツＩＤを用いて一元的に管理される。

【０５１６】サービスプロバイダ３１０は、例えば、コンテンツＩＤを用いて共通データベース８２０をブランジング（検索）して、所望のセキュアコンテナ８２１を共通データベース８２０から受けて、セキュアコンテナ８２１に、コンテンツの販売価格を示すプライスタグデータ３１２などをさらに格納したセキュアコンテナ８２２を作成し、セキュアコンテナ８２２をユーザホームネットワーク３０３に配給する。

【０５１７】ユーザホームネットワーク３０３では、オインラインの場合にはＣＡモジュール３１１を介してセキュアコンテナ８２２がＳＡＭ３０５$_1$などに提供され、ＳＡＭ３０５$_1$などにおいて、キーファイルＫＦに

176

格納されたコンテンツ鍵データＫｃおよび権利書データ１０６などが配信用鍵データＫＤ$_1$～ＫＤ$_3$などを用いて復号され、復号された権利書データ１０６に基づいて、コンテンツファイルＣＦに格納されたコンテンツデータの購入形態などの取り扱いが決定される。また、ＳＡＭ３０５$_1$などにおいて、コンテンツデータの購入履歴などを示す利用履歴データ３０８が生成され、利用履歴データ３０８がＥＭＤサービスセンタ３０２に送信される。また、ユーザホームネットワーク３０３のＳＡＭ３０５$_2$から、ユーザホームネットワーク３０３ａのＳＡＭ３０５$_{12}$にセキュアコンテナ８２２が配給された場合には、ＳＡＭ３０５$_{12}$においてＳＡＭ３０５$_2$と同様の処理が行われ、ＳＡＭ３０５$_{12}$からＥＭＤサービスセンタ３０２に利用履歴データ３０８が送信される。

【０５１８】なお、ユーザホームネットワーク３０３，３０３ａにおけるセキュアコンテナ８０７に対しての処理は、前述した第１実施形態および第２実施形態におけるユーザホームネットワーク１０３，３０３における処理と同じである。また、図１３３に示す例では、コンテンツプロバイダ３０１から共通データベース８２０、共通データベース８２０からサービスプロバイダ３１０、並びにサービスプロバイダ３１０からユーザホームネットワーク３０３に、コンテンツファイルＣＦおよびキーファイルＫＦを格納したセキュアコンテナを送る場合（イン・バンドの場合）を例示したが、コンテンツファイルＣＦおよびキーファイルＫＦを同一経路で別々に送信してもよい（アウト・オブ・バンドの場合）。また、図１３４に示すように、コンテンツプロバイダ３０１から共通データベース８２０にコンテンツファイルＣＦを格納し、サービスプロバイダ３１０が共通データベース８２０からコンテンツファイルＣＦを得ると共に、ＥＭＤサービスセンタ３０２からサービスプロバイダ３１０にキーファイルＫＦを送るようにしてもよい。この場合には、サービスプロバイダ３１０は、共通データベース８２０から得たコンテンツファイルＣＦと、ＥＭＤサービスセンタ３０２から得たキーファイルＫＦと、プライスタグデータ３１２とを格納してセキュアコンテナ８２２を作成する。共通データベース８２０は、複数のコンテンツプロバイダ３０１が提供するコンテンツデータに対してグローバルユニークに付されたコンテンツＩＤを用いて、コンテンツファイルＣＦを一元的に管理する。

【０５１９】また、図１３５に示すように、ＥＭＤサービスセンタ３０２が作成したキーファイルＫＦを、ユーザホームネットワーク３０３，３０３ａのＳＡＭ３０５$_1$，３０５$_{12}$などに送るようにしてもよい。この場合には、サービスプロバイダ３１０は、コンテンツファイルＣＦをユーザホームネットワーク３０３に配給する。プライスタグデータ３１２は、サービスプロバイダ３１０がユーザホームネットワーク３０３に配給してもよい

し、ＥＭＤサービスセンタ３０２がユーザホームネットワーク３０３，３０３ａに配給してもよい。

【０５２０】第６実施形態

図１３６は本発明の第６実施形態のＥＭＤシステムを説明するための図である

【０５２１】本実施形態のＥＭＤシステムは、前述した図１３３に示すＥＭＤシステムと比較すると、複数のＥＭＤサービスセンタ３０２を有し、コンテンツプロバイダ３０１がそれぞれ対応するＥＭＤサービスセンタ３０２との間で課金処理などを行うことを特徴としている点が異なり、それ以外の点は略同じである。コンテンツプロバイダ３０１は例えば図５（Ａ）に示すコンテンツファイルＣＦを作成する。また、コンテンツプロバイダ３０１は、複数のＥＭＤサービスセンタ３０２のう自らが選択した（あるいは予め決められた）一のＥＭＤサービスセンタ３０２に、コンテンツデータのコンテンツＩＤ、コンテンツ鍵データＫｃ、電子透かし管理情報（コンテンツデータに埋め込む電子透かし情報の内容、並びに埋め込み位置情報）、コンテンツプロバイダ３０１の識別子ＣＰ＿ＩＤ、コンテンツデータを提供するサービスプロバイダ３１０の識別子ＳＰ＿ＩＤ、コンテンツデータの卸売価格ＳＲＰを送り、ＥＭＤサービスセンタ３０２において図５（Ｂ）に示すキーファイルＫＦを作成する。ＥＭＤサービスセンタ３０２は、作成したキーファイルＫＦを、対応するコンテンツプロバイダ３０１に送る。また、ＥＭＤサービスセンタ３０２は、ＫＦデータベース１５３ａにキーファイルＫＦを格納し、個々のコンテンツデータに割り当てられたコンテンツＩＤを用いてキーファイルＫＦを一元的に管理する。このとき、コンテンツＩＤは、例えば、ＥＭＤサービスセンタ３０２によって作成され、共通データベース８３０に格納される全てのセキュアコンテナ８３１に対応するコンテンツデータを対象としてグローバルユニークに決定される。

【０５２２】次に、コンテンツプロバイダ３０１において、作成したコンテンツファイルＣＦと、ＥＭＤサービスセンタ３０２から受けたキーファイルＫＦとを格納したセキュアコンテナ８３１が作成され、セキュアコンテナ８３１が共通データベース８２０に格納される。共通データベース８３０において、複数のコンテンツプロバイダ３０１が提供したセキュアコンテナ８３１が、コンテンツＩＤを用いて一元的に管理される。

【０５２３】サービスプロバイダ３１０は、例えば、コンテンツＩＤを用いて共通データベース８２０をブランジング（検索）して、所望のセキュアコンテナ８３１を共通データベース８２０から受けて、セキュアコンテナ８３１に、コンテンツの販売価格を示すプライスタグデータ３１２などをさらに格納したセキュアコンテナ８３２を作成し、セキュアコンテナ８３２をユーザホームネットワーク３０３に配給する。

【０５２４】ユーザホームネットワーク３０３では、オインラインの場合にはＣＡモジュール３１１を介してセキュアコンテナ８３２がＳＡＭ３０５$_1$などに提供され、ＳＡＭ３０５$_1$などにおいて、キーファイルＫＦに格納されたコンテンツ鍵データＫｃおよび権利書データ１０６などが配信用鍵データＫＤ$_1$～ＫＤ$_3$などを用いて復号され、復号された権利書データ１０６に基づいて、コンテンツファイルＣＦに格納されたコンテンツデータの購入形態などの取り扱いが決定される。また、ＳＡＭ３０５$_1$などにおいて、コンテンツデータの購入履歴などを示す利用履歴データ３０８が生成され、利用履歴データ３０８がＥＭＤサービスセンタ３０２に送信される。また、ユーザホームネットワーク３０３のＳＡＭ３０５$_2$から、ユーザホームネットワーク３０３ａのＳＡＭ３０５$_{12}$にセキュアコンテナ８３２が配給された場合には、ＳＡＭ３０５$_{12}$においてＳＡＭ３０５$_2$と同様の処理が行われ、ＳＡＭ３０５$_{12}$からＥＭＤサービスセンタ３０２に利用履歴データ３０８が送信される。

【０５２５】なお、ユーザホームネットワーク３０３，３０３ａにおけるセキュアコンテナ８０７に対しての処理は、前述した第１実施形態および第２実施形態におけるユーザホームネットワーク１０３，３０３における処理と同じである。また、図１３６に示す例では、コンテンツプロバイダ３０１から共通データベース８３０、共通データベース８３０からサービスプロバイダ３１０、並びにサービスプロバイダ３１０からユーザホームネットワーク３０３に、コンテンツファイルＣＦおよびキーファイルＫＦを格納したセキュアコンテナを送る場合（イン・バンドの場合）を例示したが、コンテンツファイルＣＦおよびキーファイルＫＦを同一経路で別々に送信してもよい（アウト・オブ・バンドの場合）。また、図１３７に示すように、コンテンツプロバイダ３０１から共通データベース８３０にコンテンツファイルＣＦを格納し、サービスプロバイダ３１０が共通データベース８２０からコンテンツファイルＣＦを得ると共に、ＥＭＤサービスセンタ３０２からサービスプロバイダ３１０にキーファイルＫＦを送るようにしてもよい。このとき、サービスプロバイダ３１０が得たコンテンツファイルＣＦを作成したコンテンツプロバイダ３０１に対応するＥＭＤサービスセンタ３０２からサービスプロバイダ３１０にキーファイルＫＦが送られる。

【０５２６】サービスプロバイダ３１０は、共通データベース８３０から得たコンテンツファイルＣＦと、ＥＭＤサービスセンタ３０２から得たキーファイルＫＦと、プライスタグデータ３１２とを格納してセキュアコンテナ８３２を作成する。共通データベース８３０は、複数のコンテンツプロバイダ３０１が提供するコンテンツデータに対してグローバルユニークに付されたコンテンツＩＤを用いて、コンテンツファイルＣＦを一元的に管理

する。

【０５２７】また、図１３８に示すように、ＥＭＤサービスセンタ３０２が作成したキーファイルＫＦを、ユーザホームネットワーク３０３，３０３ａのＳＡＭ３０５$_1$，３０５$_{1,2}$などに送るようにしてもよい。このときも、ＳＡＭ３０５$_1$，３０５$_{1,2}$などに提供されたコンテンツファイルＣＦを作成したコンテンツプロバイダ３０１に対応するＥＭＤサービスセンタ３０２からＳＡＭ３０５$_1$，３０５$_{1,2}$などにキーファイルＫＦが送られる。また、サービスプロバイダ３１０は、コンテンツファイルＣＦをユーザホームネットワーク３０３に配給する。プライスタグデータ３１２は、サービスプロバイダ３１０がユーザホームネットワーク３０３に配給してもよいし、ＥＭＤサービスセンタ３０２がユーザホームネットワーク３０３，３０３ａに配給してもよい。

【０５２８】第７実施形態

図１３９は本発明の第７実施形態のＥＭＤシステムを説明するための図である。

【０５２９】本実施形態のＥＭＤシステムは、前述した図１３６に示すＥＭＤシステムと比較すると、コンテンツプロバイダ３０１からＥＭＤサービスセンタ３０２にコンテンツデータのマスタソースＳ１１１を送り、ＥＭＤサービスセンタ３０２においてコンテンツファイルＣＦを作成する点が異なり、それ以外の点は略同じである。コンテンツプロバイダ３０１は、コンテンツデータのマスタソースＳ１１１を複数のＥＭＤサービスセンタ３０２のうち自らが選択した（あるいは予め決められた）一のＥＭＤサービスセンタ３０２に送り、ＥＭＤサービスセンタ３０２において、図５（Ａ）に示すコンテンツファイルＣＦを作成する。ＥＭＤサービスセンタ３０２は、作成したコンテンツファイルＣＦを対応するコンテンツプロバイダ３０１に送る。

【０５３０】また、コンテンツプロバイダ３０１は、上記一の対応するＥＭＤサービスセンタ３０２に、コンテンツデータのコンテンツＩＤ、コンテンツ鍵データＫｃ、電子透かし管理情報（コンテンツデータに埋め込む電子透かし情報の内容）、コンテンツプロバイダ３０１の識別子ＣＰ＿ＩＤ、コンテンツデータを提供するサービスプロバイダ３１０の識別子ＳＰ＿ＩＤ、コンテンツデータの卸売価格ＳＲＰを送り、ＥＭＤサービスセンタ３０２において図５（Ｂ）に示すキーファイルＫＦを作成する。ＥＭＤサービスセンタ３０２は、作成したキーファイルＫＦを、対応するコンテンツプロバイダ３０１に送る。また、ＥＭＤサービスセンタ３０２は、ＣＦデータベース８０２ａにコンテンツファイルＣＦを格納し、ＫＦデータベース１５３ａにキーファイルＫＦを格納し、個々のコンテンツデータに割り当てられたコンテンツＩＤを用いてコンテンツファイルＣＦおよびキーファイルＫＦを一元的に管理する。このとき、コンテンツＩＤは、例えば、ＥＭＤサービスセンタ３０２によって作成され、共通データベース８４０に格納される全てのセキュアコンテナ８３１に対応するコンテンツデータを対象としてグローバルユニークに決定される。

【０５３１】次に、コンテンツプロバイダ３０１において、対応するＥＭＤサービスセンタ３０２から受けたコンテンツファイルＣＦおよびキーファイルＫＦとを格納したセキュアコンテナ８４１が作成され、セキュアコンテナ８４１が共通データベース８４０に格納される。共通データベース８４０において、複数のコンテンツプロバイダ３０１が提供したセキュアコンテナ８４１が、コンテンツＩＤを用いて一元的に管理される。

【０５３２】サービスプロバイダ３１０は、例えば、コンテンツＩＤを用いて共通データベース８４０をブランジング（検索）して、所望のセキュアコンテナ８４１を共通データベース８４０から受けて、セキュアコンテナ８４１に、コンテンツの販売価格を示すプライスタグデータ３１２などをさらに格納したセキュアコンテナ８４２を作成し、セキュアコンテナ８４２をユーザホームネットワーク３０３に配給する。

【０５３３】ユーザホームネットワーク３０３では、オインラインの場合にはＣＡモジュール３１１を介してセキュアコンテナ８４２がＳＡＭ３０５$_1$などに提供され、ＳＡＭ３０５$_1$などにおいて、キーファイルＫＦに格納されたコンテンツ鍵データＫｃおよび権利書データ１０６などが配信用鍵データＫＤ$_1$～ＫＤ$_3$などを用いて復号され、復号された権利書データ１０６に基づいて、コンテンツファイルＣＦに格納されたコンテンツデータの購入形態などの取り扱いが決定される。また、ＳＡＭ３０５$_1$などにおいて、コンテンツデータの購入履歴などを示す利用履歴データ３０８が生成され、利用履歴データ３０８がＥＭＤサービスセンタ３０２に送信される。また、ユーザホームネットワーク３０３のＳＡＭ３０５$_2$から、ユーザホームネットワーク３０３ａのＳＡＭ３０５$_{1,2}$にセキュアコンテナ８３２が配給された場合には、ＳＡＭ３０５$_{1,2}$においてＳＡＭ３０５$_2$と同様の処理が行われ、ＳＡＭ３０５$_{1,2}$からＥＭＤサービスセンタ３０２に利用履歴データ３０８が送信される。

【０５３４】なお、ユーザホームネットワーク３０３，３０３ａにおけるセキュアコンテナ８０７に対しての処理は、前述した第１実施形態および第２実施形態におけるユーザホームネットワーク１０３，３０３における処理と同じである。また、図１３９に示す例では、コンテンツプロバイダ３０１から共通データベース８４０、共通データベース８４０からサービスプロバイダ３１０、並びにサービスプロバイダ３１０からユーザホームネットワーク３０３に、コンテンツファイルＣＦおよびキーファイルＫＦを格納したセキュアコンテナを送る場合（イン・バンドの場合）を例示したが、コンテンツファイルＣＦおよびキーファイルＫＦを同一経路で別々に送

信してもよい（アウト・オブ・バンドの場合）。また、図１４０に示すように、コンテンツプロバイダ３０１から共通データベース８３０にコンテンツファイルＣＦを格納し、サービスプロバイダ３１０が共通データベース８２０からコンテンツファイルＣＦを得ると共に、ＥＭＤサービスセンタ３０２からサービスプロバイダ３１０にキーファイルＫＦを送るようにしてもよい。このとき、サービスプロバイダ３１０が得たコンテンツファイルＣＦを作成したコンテンツプロバイダ３０１に対応するＥＭＤサービスセンタ３０２からサービスプロバイダ３１０にキーファイルＫＦが送られる。

【０５３５】サービスプロバイダ３１０は、共通データベース８４０から得たコンテンツファイルＣＦと、ＥＭＤサービスセンタ３０２から得たキーファイルＫＦと、プライスタグデータ３１２とを格納してセキュアコンテナ８４２を作成する。共通データベース８３０は、複数のコンテンツプロバイダ３０１が提供するコンテンツデータに対してグローバルユニークに付されたコンテンツＩＤを用いて、コンテンツファイルＣＦを一元的に管理する。

【０５３６】また、図１４１に示すように、ＥＭＤサービスセンタ３０２が作成したキーファイルＫＦを、ユーザホームネットワーク３０３，３０３ａのＳＡＭ３０５$_1$，３０５$_{12}$などに送るようにしてもよい。このときも、ＳＡＭ３０５$_1$，３０５$_{12}$などに提供されたコンテンツファイルＣＦを作成したコンテンツプロバイダ３０１に対応するＥＭＤサービスセンタ３０２からＳＡＭ３０５$_1$，３０５$_{12}$などにキーファイルＫＦが送られる。また、サービスプロバイダ３１０は、コンテンツファイルＣＦをユーザホームネットワーク３０３に配給する。プライスタグデータ３１２は、サービスプロバイダ３１０がユーザホームネットワーク３０３に配給してもよいし、ＥＭＤサービスセンタ３０２がユーザホームネットワーク３０３，３０３ａに配給してもよい。

【０５３７】第８実施形態

図１４２は、本発明の第８実施形態のＥＭＤシステムを説明するための図である。本実施形態のＥＭＤシステムでは、例えば、コンテンツプロバイダ３０１からＥＭＤサービスセンタ３０２に提供されたマスタソースを用いてＥＭＤサービスセンタ３０２が作成した図５（Ａ）に示すコンテンツファイルＣＦ、あるいはコンテンツプロバイダ３０１が作成してＥＭＤサービスセンタ３０２に提供した図５（Ａ）に示すコンテンツファイルＣＦと、ＥＭＤサービスセンタ３０２が作成した図５（Ｂ）に示すキーファイルＫＦとが、ＥＭＤサービスセンタ３０２によってサービスプロバイダ３１０を介して、あるいは直接的にユーザホームネットワーク３０３のＳＡＭ３０５$_1$に配信される。ここで、サービスプロバイダ３１０は、コンテンツファイルＣＦの販売価格を示すプライスタグデータ３１２をユーザホームネットワーク３０３に

送ると共に、プライスタグデータ３１２をＥＭＤサービスセンタ３０２に登録して権威化する。また、サービスプロバイダ３１０は、自らを、配信事業者としてＥＭＤサービスセンタ３０２に登録する。

【０５３８】本実施形態のＥＭＤシステムでは、ユーザホームネットワーク３０３の例えばＳＡＭ３０５$_1$が、サービスプロバイダ３１０あるいはＥＭＤサービスセンタ３０２から得たコンテンツファイルＣＦおよびキーファイルＫＦを、ユーザホームネットワーク３０３内のＳＡＭ３０５$_2$および／またはユーザホームネットワーク３０３ａ内のＳＡＭ３０５$_{12}$などに配信する配信事業者となる。但し、この場合に、例えば、ＥＭＤサービスセンタ３０２は、ＳＡＭ３０５$_1$がコンテンツファイルＣＦに格納されたコンテンツデータＣを購入した後に、当該購入したコンテンツデータＣを、何らかの販売マージンを加えて販売（再配付）して利益を上げることを禁止する。本実施形態のＥＭＤシステムでは、購入形態が未決定のコンテンツデータＣ、あるいは、購入形態として再生課金が決定されているコンテンツデータＣを、販売利益マージンをとらずに再配付することを条件に、ＳＡＭ３０５$_1$がコンテンツデータＣを他のＳＡＭに複製することを許可する。なお、これを機器間再配布と呼ぶ。また、本実施形態のＥＭＤシステムでは、ＳＡＭ３０５$_1$がサービスプロバイダ３１０から配給を受けたコンテンツファイルＣＦ（あるいはセキュアコンテナ）に関しては、販売利益マージンをとらない形態での機器間売買は許可される。また、本実施形態では、ＳＡＭ３０５$_1$が、販売利益マージンをとる形態でのコンテンツデータＣの販売（配信）を行う場合には、ＳＡＭ３０５$_1$はＥＭＤサービスセンタ３０２に自らを配信事業者として登録して許諾を受けると共に、コンテンツデータＣの販売価格を示すプライスタグデータ３１２をＥＭＤサービスセンタ３０２に登録する。そして、ＳＡＭ３０５$_1$は、サービスプロバイダ３１０を介さずに、ＥＭＤサービスセンタ３０２内のＣＦデータベース８０２ａおよびＫＦデータベース１５３ａから直接的にコンテンツファイルＣＦおよびキーファイルＫＦの配給を受ける。

【０５３９】第９実施形態

図１４３は、本発明の第９実施形態のＥＭＤシステムを説明するための図である。本実施形態のＥＭＤシステムでは、コンテンツプロバイダ３０１のそれぞれが、コンテンツプロバイダとしての役割に加えて、ＥＭＤサービスセンタ３０２としての役割を果たすことを特徴としてる。おの場合に、複数のコンテンツプロバイダ３０１がある場合に、それぞれのコンテンツプロバイダ３０１は、それぞれのＥＭＤサービスセンタ３０２としての役割を持つ。コンテンツプロバイダ３０１は、コンテンツファイルＣＦおよびキーファイルＫＦを格納したセキュアコンテナ８５１をサービスプロバイダ３１０に配信する。サービスプロバイダ３１０は、セキュアコンテナ８

183

５１が格納したコンテンツファイルＣＦ、キーファイルＫＦに、さらにプライスタグデータ３１２を加えてセキュアコンテナ８５２を作成し、これをユーザホームネットワーク３０３に配信する。ユーザホームネットワーク３０３，３０３ａでは、キーファイルＫＦ内に格納された権利書データ１０６に基づいてコンテンツファイルＣＦの購入形態などを決定し、それに応じた利用履歴データ３０８を作成し、これをコンテンツプロバイダ３０１内のＥＭＤサービスセンタ３０２に送信する。このとき、利用履歴データ３０８は、コンテンツプロバイダ３０１毎に作成される。コンテンツプロバイダ３０１のＥＭＤサービスセンタ３０２は、利用履歴データ３０８に基づいて、ＳＡＭ３０５$_1$，３０５$_{1\,2}$のユーザが支払った利益を、自らと対応するサービスプロバイダ３１０との間で分配する。また、ユーザホームネットワーク３０３のＣＡモジュール３１１から、配信サービスに関しての履歴データが対応するサービスプロバイダ３１０に送られ、サービスプロバイダ３１０において配信サービスに対しての課金処理が行われる。

【０５４０】本発明は上述した実施形態には限定されない。上述した実施形態では、コンテンツデータとしてオーディオデータを用いる場合を例示したが、コンテンツデータとして、ビデオデータ、オーディオ・ビデオデータ、テキストデータおよびコンピュータプログラムなどを用いてもよい。また、上述した実施形態では、ＥＭＤサービスセンタ１０２，３０２において、キーファイルＫＦを作成する場合を例示したが、コンテンツプロバイダ１０１，３０１においてキーファイルＫＦを作成することも可能である。この場合に、図７に対応するキーファイルＫＦのフォーマットは、図１４４に示すようになる。図１４４に示すように、当該キーファイルＫＦは、コンテンツプロバイダ１０１，３０１の秘密鍵データＫ$_{CP,S}$を用いて作成された署名データが用いられる点を除いて、図７に示すキーファイルＫＦと基本的に同じ情報を有している。

【０５４１】また、上述した実施形態では、ユーザホームネットワーク１０３，３０３からＥＭＤサービスセンタ１０２，３０２に、利用制御状態データ１６６をリアルタイムで送信する場合を例示したが、利用制御状態データ１６６をコンテンツプロバイダ１０１，３０１および／またはサービスプロバイダ３１０に送信するようにしてもよい。これにより、コンテンツプロバイダ１０１，３０１およびサービスプロバイダ３１０は、自らが提供および配給したコンテンツの購入状況を即座に把握でき、その後のサービスに反映できる。

【０５４２】以下、上述した本実施形態のＥＭＤシステムによる効果を、従来技術およびその問題点を述べながら再び説明する。デジタル放送（データ放送）、インターネットなどのデジタルネットワークが発達していない時代に、デジタルコンテンツ（コンテンツデータ）を流

184

用させる手段として使用されていたＲＯＭ型記録媒体では、デジタルコンテンツを非暗号化の状態で記録して流用させていた。デジタルネットワークが発達していない時代では、これらのコンテンツの著作権保護をおこなうのは、ユーザホームネットワーク上でのユーザによるカジュアルコピーを防ぐ方法を考えるだけで良かった。

【０５４３】しかしながら、デジタルネットワークが発達してきた昨今では、非暗号化コンテンツが搭載されているＲＯＭ型記録媒体を一般市民が、いつ、どこででも、自由に入手することができるために、各自がこれらを購入し、圧縮してネットワークにアップロードすることが簡単にできてしまう。特にインターネットは世界中につながっているネットワークなので、非暗号化コンテンツを無料でインターネット上にアップロードし、市民はそれを無料で自分の個人端末にダウンロードすることが可能となってしまい、コンテンツの権利者（コンテンツプロバイダ）の著作権を著しく侵害する可能性が出てきている。

【０５４４】また、非暗号化の状態でアップロードせず、自らが、そのコンテンツに対し、独自方式の電子透かし情報を埋め込み、暗号化をおこなうことで独自方式の課金機能を備え、インターネット上で著作権の許可なしに、目の届かないところで勝手に、デジタルコンテンツの販売をおこなうことも可能となっている。このときは、売り上げの一部がコンテンツの権利者に還元されないので、コンテンツの権利者（コンテンツプロバイダ）の著作権を著しく侵害することになる。また、著作権者の許諾を得て、売り上げの一部をコンテンツの権利者（コンテンツプロバイダ）に還元する契約を権利者側と事前におこなうことで、これらのデジタルコンテンツを配信して利益が得られる配信サービスをおこなうことが可能になるが、基本的にコンテンツプロバイダは、こういったコンテンツの２次利用による流通体系をあまり好ましく思っていない。コンテンツの２次利用によるビジネスとは、たとえばレンタルビジネス、中古販売などが相当する。２次利用による配信サービスが登場する時は、必ず著作権侵害の問題が起こり、サービス自体を軌道に載せるまで時間がかかる。コンテンツプロバイダと事前契約をおこなうことなしに、まず配信サービスを始めてしまい、著作権侵害ということで問題になってから、権利者側への利益分配なり著作権保護が考慮され配信サービスとしての許諾が得られる。レンタルＣＤ、レンタルビデオが相当する。ゲームソフトの中古販売などは深刻な問題である。現在ゲームソフトの中古販売ビジネスでは、売り上げの利益の一部がコンテンツの権利者側に還元されないので、権利者側は裁判で告訴しているが却下され、権利者側にとって非常に酷になっている。新作ソフトの半額以下で大量に販売されるので、ユーザからしても魅力がある市場で、新作ソフトの売り上げにも影響を及ぼす。

185

【０５４５】コンテンツの２次利用というのは、本来コンテンツの権利者がＲＯＭ型記録媒体を流通手段とし、そのデジタルコンテンツ記録済のＲＯＭ型記録媒体を商品として流通させて利益を得ている訳で、それらを購入したユーザによって、その商品をさらに流通させることで、購入したユーザが利益を得ることは、たとえ利益の一部が還元されたとしても、（コンテンツプロバイダ）権利者側の立場からするとあまり好ましく思わない。映画コンテンツなどは、録音権／領布権というものがコンテンツの権利者側に法律で保障されており、権利者が世に流通させたコンテンツを、それを購入した時点で、その購入ユーザの手元からは流通しないことを前提としている。ゲームソフトの権利者団体は、この領布権の権利をゲームソフトにも利用し、２次利用ビジネスの抑制を裁判で訴えている。

【０５４６】コンテンツの権利者は、自分が著作権を持っているデジタルコンテンツについては、それを流用させる流通業者を管理下においておきたい（誰に流通させているか、を知っておきたい）。自分が著作権を持っているデジタルコンテンツを流通させて配信サービスをおこない利益を得ることを希望している配信事業者がいる場合は、コンテンツの権利者から直接デジタルコンテンツを渡せるようなシステムが望ましい。なお、ここで述べている流通業者とは、デジタルコンテンツの対価に、さらに何％かの利益マージンを徴収することで利益を得る業者を指す。デジタルコンテンツを他機器／記録媒体へ渡すときに利益マージンを徴収する場合、そのコンテンツ売買セッション配信サービスとして定義し、利益マージンを徴収しない場合を機器間再配付として定義し、これは超流通の原理により合法である。コンテンツプロバイダが流通させた非暗号化コンテンツが記録されているＲＯＭ型記録媒体からサービスプロバイダが、自分の配信サービス用コンテンツをオーサリングし、配信サービスをおこなう現状のデジタルコンテンツのネットワーク流通管理システムにおいて、コンテンツプロバイダが所有している一つのデジタルコンテンツが複数のサービスプロバイダによって配信される状況を考えると、同一コンテンツであるにも関わらず、各々のサービスプロバイダが採用するＣＡモジュール／電子決済ツールにて権利処理がおこなわれるようにオーサリングされるため、使用される暗号鍵（コンテンツ鍵データ）、コンテンツの使用許諾条件（権利書データ）のフォーマットが各サービスプロバイダによって各々異なり、ユーザホームネットワーク上で共通の権利処理ルールを提供することができない。こういった場合では、ＣＡモジュール／電子決済ツールで利用する鍵データ類をすべてネットワーク機器のＣＡモジュール／電子決済ツールで清算し、あとはＳＣＭＳのルールに準拠することでユーザホームネットワーク上での共通の権利処理ルールを実現している。また、ＣＡモジュール／電子決済ツールの鍵で暗号化された

186

コンテンツと鍵データを、そのままネットワーク機器を通過してユーザホームネットワークバス（ＩＥＥＥ１３９４など。）を経由してストレージ機器の記録媒体に記録し、１３９４バス上につながる機器から遠隔的にネットワーク機器を経由してコンテンツの購入、決済処理ができたとしても、暗号化コンテンツを復号するためのデスクランブラがネットワーク機器に存在するので、結局再生時にネットワーク機器まで、コンテンツと鍵データを戻さないと再生できない（ネットワークＣＡ）。

【０５４７】上述したように、現在までに世の中に広く流通している非暗号化コンテンツが記録されているＲＯＭ型記録媒体の存在が、現状のデジタルコンテンツネットワーク配信サービスにとって問題の根源となっている。デジタルコンテンツのコンテンツ形態が、コンテンツプロバイダ以外の第３者によって作成される可能性を持っており、さらに、ユーザに対して、そのコンテンツを販売した人が、その対価を入手するシステムであるため、コンテンツの２次利用などコンテンツプロバイダの利益が不当に損なわれる可能がある。また、オーサリングしたデジタルコンテンツの流通管理をコンテンツプロバイダが厳密におこなっていないため、自分が著作権を持っているデジタルコンテンツが稼ぎ出す全利益、およびそこから自分の利益分が還元されているかどうかを監視することが難しい。

【０５４８】前述した本実施形態のＥＭＤシステムは、上述したような従来の問題を解決した。すなわち、本実施形態のＥＭＤシステムでは、コンテンツプロバイダがオーサリングしたデジタルコンテンツは、すべてコンテンツプロバイダ側で、コンテンツ形態や権利書データを作成し、コンテンツプロバイダ側のデータベースに管理しておく。コンテンツの権利書データに関しては、さらに第３の信頼機関であるＥＭＤサービスセンタ（クリアリングハウス）で権威化し登録しておく。こうすることで、コンテンツプロバイダの関係者が、デジタルコンテンツの権利処理ルールを完全に自分の管理下におくことができ、流通経路をコンテンツプロバイダ側で管理することを可能とする。また本件では、このコンテンツプロバイダ側で作成した権利書のデータの内容を、ユーザとの間に存在する流通業者が見ることができないような仕掛けを提供する。また、本実施形態のＥＭＤシステムでは、ＲＯＭ型記録媒体を、ひとつの流通手段として考えて、そこに搭載するデジタルコンテンツの存在をＲＯＭ型記録媒体から遊離させる。流通手段、流通経路によらず、デジタルコンテンツ単体で、その存在価値を表現するコンテンツ形態を提案する。デジタルコンテンツはコンテンツプロバイダ側である規定の形式で管理されるので、ＲＯＭ型記録媒体に、その形式のデジタルコンテンツを搭載すると考えることで、ＲＯＭ型記録媒体で流通されようが、デジタルネットワークで流通されようが、ユーザホームネットワーク上では、ＲＯＭ→ＲＡＭ、ネ

ットワーク→ＲＡＭにおいて共通の権利処理ルールを提供することが可能となる。デジタルコンテンツの販売セッションを、すべてコンテンツプロバイダが規定、管理する形式でおこなう。これにより、流通手段、流通経路によらない共通の権利処理が可能となる。また、このコンテンツプロバイダ側で規定されたコンテンツ形態は、デジタルコンテンツの売買をおこなう上での最小単位と定義することで、その後の流通過程で利用されるコンテンツ形態の種類に依存せず共通の権利処理ルールを提供することができる。ユーザホームネットワークで購入したときに生成される課金情報を、サービスプロバイダに返すのではなく、第３の信頼機関であるＥＭＤサービスセンタに返し、そこからサービスプロバイダに返すことによりコンテンツの２次利用によるビジネスの問題点を解決した。

【０５４９】

【発明の効果】以上説明したように、本発明によれば、データ提供装置が提供したコンテンツデータのデータ処理装置における取り扱いを、データ提供装置による権利書データに基づいて行わせることが可能になる。その結果、データ提供装置の関係者によるコンテンツデータに係わる利益を適切に保護することが可能になると共に、当該関係者による監査の負担を軽減できる。

【図面の簡単な説明】

【図１】図１は、本発明の第１実施形態のＥＭＤシステムの全体構成図である。

【図２】図２は、本発明のセキュアコンテナの概念を説明するための図である。

【図３】図３は、図１に示すコンテンツプロバイダの機能ブロック図であり、ユーザホームネットワークのＳＡＭとの間で送受信されるデータに関連するデータの流れを示す図である。

【図４】図４は、図１に示すコンテンツプロバイダの機能ブロック図であり、コンテンツプロバイダとＥＭＤサービスセンタとの間で送受信されるデータに関連するデータの流れを示す図である。

【図５】図５は、図１に示すコンテンツプロバイダからＳＡＭに送信されるセキュアコンテナのフォーマットを説明するための図である。

【図６】図６は、図５に示すコンテンツファイルに含まれるデータを詳細に説明するための図である。

【図７】図７は、図５に示すキーファイルに含まれるデータを詳細に説明するための図である。

【図８】図Ａ８は、コンテンツファイルに格納されるヘッダデータを説明するための図である。

【図９】図９は、コンテンツＩＤを説明するための図である。

【図１０】図１０は、セキュアコンテナのディレクトリ構造を説明するための図である。

【図１１】図１１は、セキュアコンテナのハイパーリンク構造を説明するための図である。

【図１２】図１２は、本実施形態で用いられるＲＯＭ型の記録媒体の第１の例を説明するための図である。

【図１３】図１３は、本実施形態で用いられるＲＯＭ型の記録媒体の第２の例を説明するための図である。

【図１４】図１４は、本実施形態で用いられるＲＯＭ型の記録媒体の第３の例を説明するための図である。

【図１５】図１５は、本実施形態で用いられるＲＡＭ型の記録媒体の第１の例を説明するための図である。

【図１６】図１６は、本実施形態で用いられるＲＡＭ型の記録媒体の第２の例を説明するための図である。

【図１７】図１７は、本実施形態で用いられるＲＡＭ型の記録媒体の第３の例を説明するための図である。

【図１８】図１８は、コンテンツプロバイダからＥＭＤサービスセンタに送信される登録要求用モジュールを説明するための図である。

【図１９】図１９は、コンテンツプロバイダからＥＭＤサービスセンタへの登録処理の手順を示すフローチャートである。

【図２０】図２０は、コンテンツプロバイダにおける説明の作成処理の手順を示すフローチャートである。

【図２１】図２１は、コンテンツプロバイダにおける説明の作成処理の手順を示すフローチャートである。

【図２２】図２２は、コンテンツプロバイダにおける説明の作成処理の手順を示すフローチャートである。

【図２３】図２３は、図１に示すＥＭＤサービスセンタの機能ブロック図であり、コンテンツプロバイダとの間で送受信されるデータに関連するデータの流れを示す図である。

【図２４】図２４は、図１に示すＥＭＤサービスセンタの機能ブロック図であり、ＳＡＭおよび図１に示す決済機関との間で送受信されるデータに関連するデータの流れを示す図である。

【図２５】図２５は、図１に示すユーザホームネットワーク内のネットワーク機器の構成図である。

【図２６】図２６は、図１に示すユーザホームネットワーク内のＳＡＭの機能ブロック図であり、コンテンツプロバイダから受信したセキュアコンテナを復号するまでのデータの流れを示す図である。

【図２７】図２７は、図２５に示す外部メモリに記憶されるデータを説明するための図である。

【図２８】図２８は、スタックメモリに記憶されるデータを説明するための図である。

【図２９】図２９は、図１に示すユーザホームネットワーク内のネットワーク機器のその他の構成図である。

【図３０】図３０は、図２６に示す記憶部に記憶されるデータを説明するための図である。

【図３１】図３１は、図１に示すユーザホームネットワーク内のＳＡＭの機能ブロック図であり、コンテンツデータを利用・購入する処理などに関連するデータの流れ

を示す図である。

【図３２】図３２は、図２５に示すネットワーク機器のダウンロードメモリにダウンロードされた既に購入形態が決定されたコンテンツファイルを、ＡＶ機器のＳＡＭに転送する場合の転送元のＳＡＭ内での処理の流れを説明するための図である。

【図３３】図３３は、図３２に示す場合における転送元のＳＡＭ内でのデータの流れを示す図である。

【図３４】図３４は、購入形態が決定したセキュアコンテナのフォーマットを説明するための図である。

【図３５】図３５は、図３２に示す場合において、転送先のＳＡＭにおいて、入力したコンテンッファイルなどを、ＲＡＭ型あるいはＲＯＭ型の記録媒体（メディア）に書き込む際のデータの流れを示す図である。

【図３６】図３６、コンテンツの購入形態が未決定の図７に示すＲＯＭ型の記録媒体をユーザホームネットワークがオフラインで配給を受けた場合に、ＡＶ機器において購入形態を決定する際の処理の流れを説明するための図である。

【図３７】図３７は、図３６に示す場合において、ＳＡＭ内でのデータの流れを示す図である。

【図３８】図３８は、ユーザホームネットワーク内のＡＶ機器において購入形態が未決定のＲＯＭ型の記録媒体からセキュアコンテナを読み出して、これを他のＡＶ機器に転送してＲＡＭ型の記録媒体に書き込む際の処理の流れを説明するための図である。

【図３９】図３９は、図３８に示す場合における転送元のＳＡＭ内でのデータの流れを示す図である。

【図４０】図４０は、図３８において、転送元のＳＡＭから転送先のＳＡＭに転送されるセキュアコンテナのフォーマットを説明するための図である。

【図４１】図４１は、図３８に示す場合における転送先のＳＡＭ内でのデータの流れを示す図である。

【図４２】図４２は、図１に示すコンテンツプロバイダ、ＥＭＤサービスセンタおよびＳＡＭの相互間で、イン・バント方式およびアウト・オブ・バンド方式で、送受信されるデータのフォーマットを説明するための図である。

【図４３】図４３は、図１に示すコンテンツプロバイダ、ＥＭＤサービスセンタおよびＳＡＭの相互間で、イン・バント方式およびアウト・オブ・バンド方式で、送受信されるデータのフォーマットを説明するための図である。

【図４４】図４４は、ユーザホームネットワーク内でのバスへの機器の接続形態の一例を説明するための図である。

【図４５】図４５は、ＳＡＭが作成するＳＡＭ登録リストのデータフォーマットを説明するための図である。

【図４６】図４６は、ＥＭＤサービスセンタが作成するＳＡＭ登録リストのデータフォーマットを説明するための図である。

【図４７】図４７は、図１に示すコンテンツプロバイダの全体動作のフローチャートである。

【図４８】図４８は、第１実施形態のＥＭＤシステムにおいて用いられるセキュアコンテナの配送プロトコルの一例を説明するための図である。

【図４９】図４９は、本発明の第１実施形態の第２変形例を説明するための図である。

【図５０】図５０は、本発明の第１実施形態の第３変形例を説明するための図である。

【図５１】図５１は、本発明の第１実施形態の第４変形例において第１の手法を採用した場合を説明するための図である。

【図５２】図５２は、本発明の第１実施形態の第４変形例において第２の手法を採用した場合を説明するための図である。

【図５３】図５３は、本発明の第１実施形態の第５変形例を説明するための図である。

【図５４】図５４は、本発明の第１実施形態の第６変形例の第１のパターンを説明するための図である。

【図５５】図５５は、本発明の第１実施形態の第６変形例の第２のパターンを説明するための図である。

【図５６】図５６は、本発明の第１実施形態の第６変形例の第３のパターンを説明するための図である。

【図５７】図５７は、本発明の第１実施形態の第６変形例の第４のパターンを説明するための図である。

【図５８】図５８は、本発明の第１実施形態の第６変形例の第５のパターンを説明するための図である。

【図５９】図５９は、本発明の第２実施形態のＥＭＤシステムの全体構成図である。

【図６０】図６０は、図５９に示すコンテンツプロバイダの機能ブロック図であり、サービスプロバイダに送信されるセキュアコンテナに関するデータの流れを示す図である。

【図６１】図６１は、コンテンツプロバイダにおいて行われるセキュアコンテナの配送処理の手順を示すフローチャートである。

【図６２】図６２は、コンテンツプロバイダにおいて行われるセキュアコンテナの配送処理の手順を示すフローチャートである。

【図６３】図６３は、図５９に示すサービスプロバイダの機能ブロック図であり、ユーザホームネットワークとの間で送受信されるデータの流れを示す図である。

【図６４】図６４は、サービスプロバイダにおいて行われるセキュアコンテナの作成処理の手順を示すフローチャートである。

【図６５】図６５は、図５９に示すサービスプロバイダからユーザホームネットワークに送信されるセキュアコンテナのフォーマットを説明するための図である。

【図６６】図６６は、図６５に示すセキュアコンテナに

格納されたコンテンツファイルの送信形態を説明するための図である。

【図６７】図６７は、図６５に示すセキュアコンテナに格納されたキーファイルの送信形態を説明するための図である。

【図６８】図６８は、図５９に示すサービスプロバイダの機能ブロック図であり、ＥＭＤサービスセンタとの間で送受信されるデータの流れを示す図である。

【図６９】図６９は、サービスプロバイダからＥＭＤサービスセンタに送信されるプライスタグ登録要求用モジュールのフォーマットを説明するための図である。

【図７０】図７０は、図５９に示すＥＭＤサービスセンタの機能ブロック図であり、サービスプロバイダとの間で送受信されるデータに関連するデータの流れを示す図である。

【図７１】図７１は、図５９に示すＥＭＤサービスセンタの機能ブロック図であり、コンテンツプロバイダとの間で送受信されるデータに関連するデータの流れを示す図である。

【図７２】図７２は、図５９に示すＥＭＤサービスセンタの機能ブロック図であり、ＳＡＭとの間で送受信されるデータに関連するデータの流れを示す図である。

【図７３】図７３は、利用履歴データの内容を説明するための図である。

【図７４】図７４は、図５９に示すネットワーク機器の構成図である。

【図７５】図７５は、図７４に示すＣＡモジュールの機能ブロック図である。

【図７６】図７６は、図７４に示すＳＡＭの機能ブロック図であり、セキュアコンテナを入力してから復号するまでのデータの流れを示す図である。

【図７７】図７７は、図７６に示す記憶部に記憶されるデータを説明するための図である。

【図７８】図７８は、図７４に示すＳＡＭの機能ブロック図であり、コンテンツの購入・利用形態を決定する場合などのデータの流れを示す図である。

【図７９】図７９は、ＳＡＭにおけるセキュアコンテナの購入形態の決定処理の手順を示すフローチャートである。

【図８０】図８０は、購入形態が決定された後のキーファイルのフォーマットを説明するための図である。

【図８１】図８１は、図７４に示すネットワーク機器のダウンロードメモリにダウンロードされた既に購入形態が決定されたコンテンツファイルを、ＡＶ機器のＳＡＭに転送する場合の転送先のＳＡＭ内での処理の流れを説明するための図である。

【図８２】図８２は、図８１に示す場合の転送元のＳＡＭ内でのデータの流れを示す図である。

【図８３】図８３は、図８１に示す場合の転送先のＳＡＭ内でのデータの流れを示す図である。

【図８４】図８４は、図５９に示すＥＭＤシステムの全体動作のフローチャートである。

【図８５】図８５は、図５９に示すＥＭＤシステムの全体動作のフローチャートである。

【図８６】図８６は、第２実施形態のＥＭＤシステムにおけるサービスプロバイダからユーザホームネットワークへのセキュアコンテナの配送形態の一例を説明するための図である。

【図８７】図８７は、第２実施形態のＥＭＤシステムが採用するセキュアコンテナの配送プロトコルの一例を説明するための図である。

【図８８】図８８は、図８７においてユーザホームネットワークからサービスプロバイダ３１０へのセキュアコンテナなどを配送する際に用いられる配送プロトコルを説明するための図である。

【図８９】図８９は、図８７においてコンテンツプロバイダからＥＭＤサービスセンタへのキーファイルなどを配送する際に用いられる配送プロトコルを説明するための図である。

【図９０】図９０は、図８７においてサービスプロバイダからＥＭＤサービスセンタへのプライスタグデータ３１２などを配送する際に用いられる配送プロトコルを説明するための図である。

【図９１】図９１は、図８７においてユーザホームネットワーク内でセキュアコンテナなどを配送する際に用いられる配送プロトコルを説明するための図である。

【図９２】図９２は、デジタル放送のデータ放送方式にＸＭＬ／ＳＭＩＬ／ＢＭＬを利用した場合のプロトコル層へのセキュアコンテナのインプリメント形態を説明するための図である。

【図９３】図９３は、デジタル放送のデータ放送方式にＭＨＥＧを利用した場合のプロトコル層へのセキュアコンテナのインプリメント形態を説明するための図である。

【図９４】図９４は、インターフェイスのデータ放送方式にＸＭＬ／ＳＭＩＬを利用した場合のプロトコル層へのセキュアコンテナのインプリメント形態を説明するための図である。

【図９５】図９５は、ユーザホームネットワークからＥＭＤサービスセンタに利用履歴データなどを配送する際に用いられる配送プロトコルを説明するための図である。

【図９６】図９６は、ユーザホームネットワーク内においてセキュアコンテナなどを配送する際に用いられる配送プロトコルを説明するための図である。

【図９７】図９７は、本発明の第２実施形態の第１変形例に係わる２個のサービスプロバイダを用いたＥＭＤシステムの構成図である。

【図９８】図９８は、本発明の第２実施形態の第２変形例に係わる複数のコンテンツプロバイダを用いたＥＭＤ

システムの構成図である。

【図９９】図９９は、本発明の第２実施形態の第３変形例に係わるＥＭＤシステムの構成図である。

【図１００】図１００は、本発明の第２実施形態の第４変形例に係わるＥＭＤシステムの構成図である。

【図１０１】図１０１は、公開鍵証明書データの取得ルートの形態を説明するための図である。

【図１０２】図１０２は、コンテンツプロバイダの公開鍵証明書データを無効にする場合の処理を説明するための図である。

【図１０３】図１０３は、サービスプロバイダの公開鍵証明書データを無効にする場合の処理を説明するための図である。

【図１０４】図１０４は、ＳＡＭの公開鍵証明書データを無効にする場合の処理を説明するための図である。

【図１０５】図１０５は、ＳＡＭの公開鍵証明書データを無効にする場合のその他の処理を説明するための図である。

【図１０６】図１０６は、図４７に示すＥＭＤシステムにおいて、ＥＭＤサービスセンタの代わりに権利管理用クリアリングハウスおよび電子決済用クリアリングハウスを設けた場合を説明するための図である。

【図１０７】図１０７は、図１０６に示す権利管理用クリアリングハウスおよび電子決済用クリアリングハウスを単体のＥＭＤサービスセンタ内に設けた場合のＥＭＤシステムの構成図である。

【図１０８】図１０８は、サービスプロバイダが電子決済用クリアリングハウスに直接的に決済を行う場合のＥＭＤシステムの構成図である。

【図１０９】図１０９は、コンテンツプロバイダが電子決済用クリアリングハウスに直接的に決済を行う場合のＥＭＤシステムの構成図である。

【図１１０】図１１０は、コンテンツプロバイダが権利管理用クリアリングハウスおよび電子決済用クリアリングハウスの双方の機能をさらに備えている場合のＥＭＤシステムの構成図である。

【図１１１】図１１１は、本発明の第２実施形態の第８変形例において、図４７に示すコンテンツプロバイダからサービスプロバイダに提供されるセキュアコンテナのフォーマットを説明するための図である。

【図１１２】図１１２は、図１１１に示すコンテンツファイルとキーファイルとの間のディレクトリ構造データによるリンク関係を説明するための図である。

【図１１３】図１１３は、コンテンツファイルとキーファイルとの間のディレクトリ構造のその他の例を説明するための図である。

【図１１４】図１１４は、本発明の第２実施形態の第８変形例において、図４７に示すサービスプロバイダからＳＡＭに提供されるセキュアコンテナのフォーマットを説明するための図である。

【図１１５】図１１５は、コンポジット型のセキュアコンテナのデータフォーマットの第１の概念を説明するための図である。

【図１１６】図１１６は、コンポジット型のセキュアコンテナのデータフォーマットの第２の概念を説明するための図である。

【図１１７】図１１７は、本発明の第２実施形態の第８変形例に係わるＥＭＤシステムにおいて第１の手法を採用した場合を説明するための図である。

【図１１８】図１１８は、本発明の第２実施形態の第８変形例に係わるＥＭＤシステムにおいて第２の手法を採用した場合を説明するための図である。

【図１１９】図１１９は、本発明の第２実施形態の第８変形例に係わるＥＭＤシステムにおいてファイル形式を採用しない場合のデータフォーマットを説明するための図である。

【図１２０】図１２０は、本発明の第２実施形態の第１０変形例に係わるＥＭＤシステムの構成図である。

【図１２１】図１２１は、本発明の第２実施形態の第１１変形例の第１のパターンに係わるＥＭＤシステムの構成図である。

【図１２２】図１２２は、本発明の第２実施形態の第１１変形例の第２のパターンに係わるＥＭＤシステムの構成図である。

【図１２３】図１２３は、本発明の第２実施形態の第１１変形例の第３のパターンに係わるＥＭＤシステムの構成図である。

【図１２４】図１２４は、本発明の第２実施形態の第１１変形例の第４のパターンに係わるＥＭＤシステムの構成図である。

【図１２５】図１２５は、本発明の第２実施形態の第１１変形例の第５のパターンに係わるＥＭＤシステムの構成図である。

【図１２６】図１２６は、本発明の第２実施形態の第９変形例に係わるＥＭＤシステムの構成図である。

【図１２７】図１２７は、本発明の第２実施形態におけるセキュアコンテナのファイル包括大小関係を説明するための図である。

【図１２８】図１２８は、本発明の第３実施形態のＥＭＤシステムを説明するための図である。

【図１２９】図１２９は、図１２８に示すＥＭＤサービスセンタの機能ブロック図である。

【図１３０】図１３０は、本発明の第３実施形態のＥＭＤシステムの変形例を説明するための図である。

【図１３１】図１３１は本発明の第４実施形態のＥＭＤシステムを説明するための図である。

【図１３２】図１３２は本発明の第４実施形態のＥＭＤシステムの変形例を説明するための図である。

【図１３３】図１３３は本発明の第５実施形態のＥＭＤシステムを説明するための図である。

195

【図１３４】図１３４は本発明の第５実施形態のＥＭＤシステムの変形例を説明するための図である。

【図１３５】図１３５は本発明の第５実施形態のＥＭＤシステムのその他の変形例を説明するための図である。

【図１３６】図１３６は本発明の第６実施形態のＥＭＤシステムを説明するための図である。

【図１３７】図１３７は本発明の第６実施形態のＥＭＤシステムの変形例を説明するための図である。

【図１３８】図１３８は本発明の第６実施形態のＥＭＤシステムのその他の変形例を説明するための図である。

【図１３９】図１３９は本発明の第７実施形態のＥＭＤシステムを説明するための図である。

【図１４０】図１４０は本発明の第７実施形態のＥＭＤシステムの変形例を説明するための図である。

【図１４１】図１４１は本発明の第７実施形態のＥＭＤシステムのその他の変形例を説明するための図である。

【図１４２】図１４２は本発明の第８実施形態のＥＭＤシステムを説明するための図である。

【図１４３】図１４３は本発明の第９実施形態のＥＭＤシステムを説明するための図である。

196

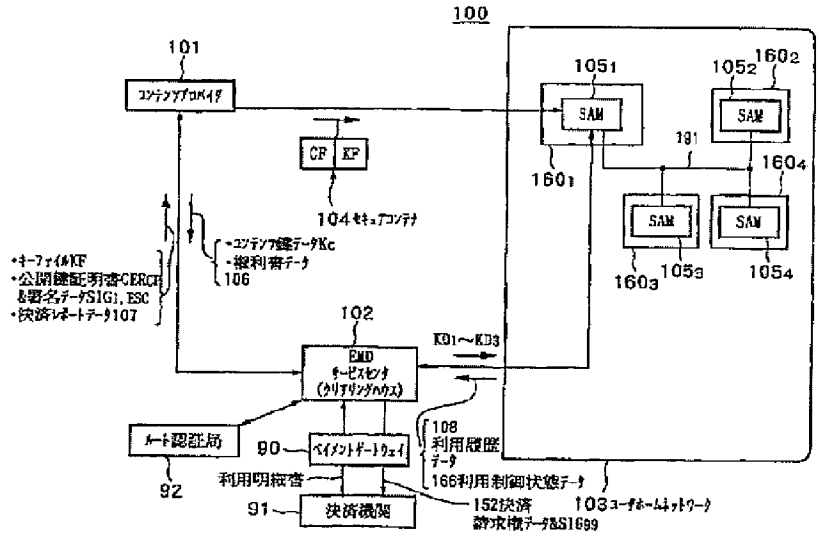
【図１４４】図１４４は、コンテンツプロバイダにおいてキーファイルを作成した場合のキーファイルのフォーマットを説明するための図である。

【図１４５】図１４５は、従来のＥＭＤシステムの構成図である。

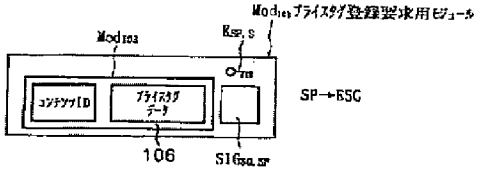
【符号の説明】

９０…ペイメントゲートウェイ、９１…決済機関、９２…ルート認証局、１００，３００…ＥＭＤシステム、１０１，３０１…コンテンツプロバイダ、１０２，３０２…ＥＭＤサービスセンタ、１０３，３０３…ユーザホームネットワーク、１０４，３０４…セキュアコンテナ、105_1～105_4，305_1～305_4…ＳＡＭ、１０６…権利書データ、１０７，３０７…決済レポートデータ、１０８，３０８…利用履歴データ、160_1…ネットワーク機器、160_2～160_4…ＡＶ機器、１５２，１５２ｃ，１５２ｓ…決済請求権データ、１９１…バス、３１０…サービスプロバイダ、３１１…ＣＡモジュール、３１２…プライスタグデータ、ＣＦ…コンテンツファイル、ＫＦ…キーファイル、Ｋｃ…コンテンツ鍵データ

【図１】



【図６９】



【図２７】

外部メモリ201に記憶されるデータ

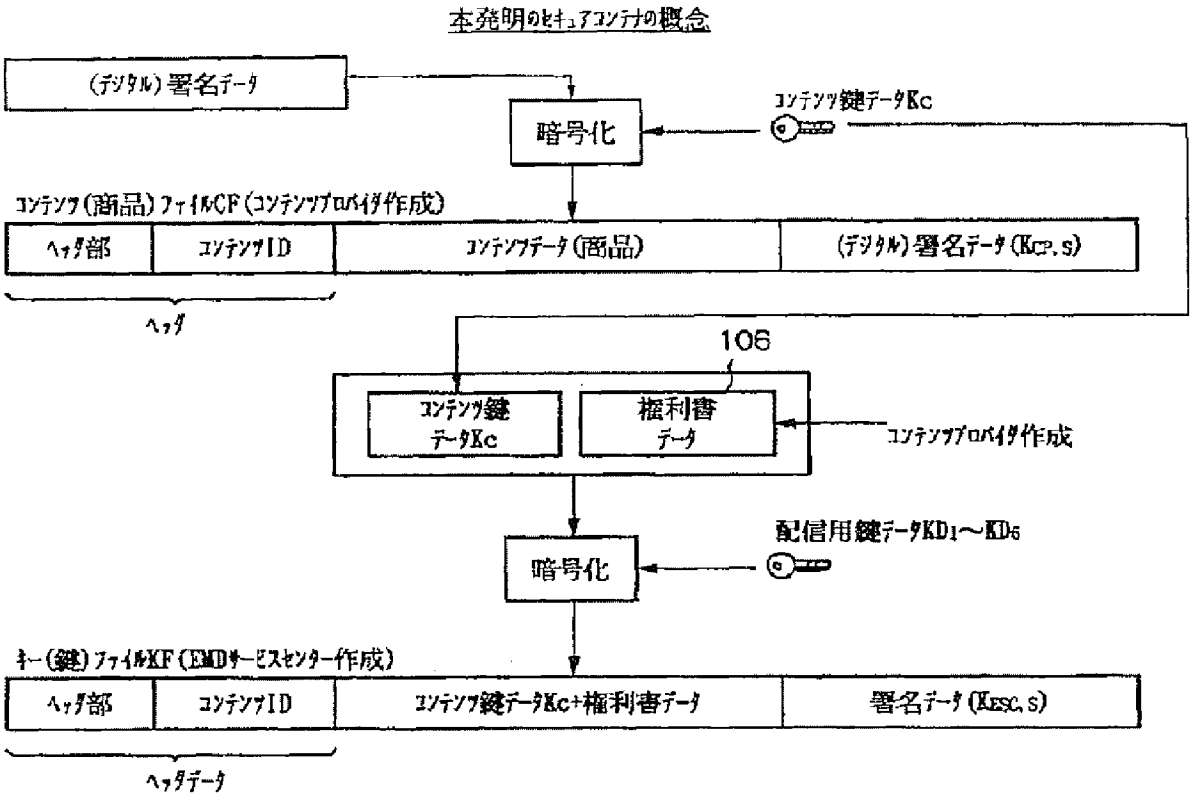
利用履歴データ108
SAM登録リスト

【図７３】

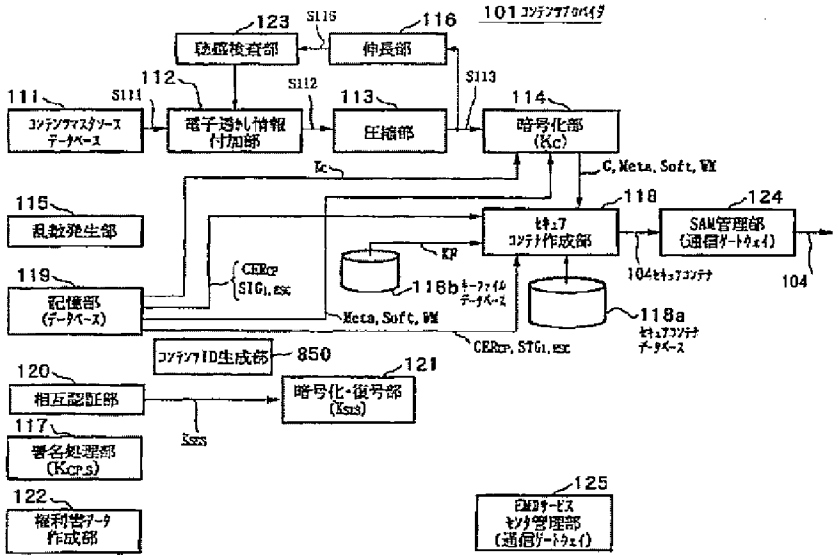
利用履歴データ308の内容

識別子Content_ID
識別子CP_ID
識別子SP_ID
コンテンツデータCの信号諸元データ
コンテンツデータCの圧縮方法
記録媒体の識別子Media_ID
識別子SAM_ID、
ユーザのUSER_ID

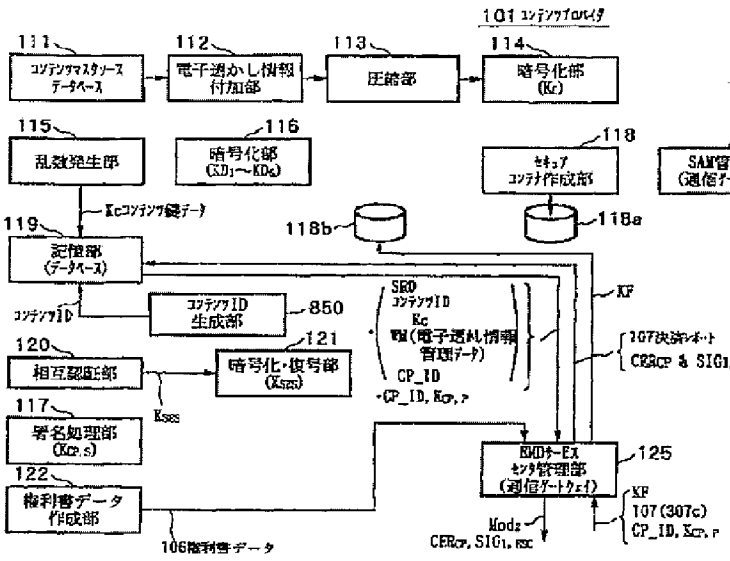
【図２】


本発明のセキュアコンテナの概念
(デジタル)署名データ
暗号化
コンテンツ鍵データKc
コンテンツ(商品)ファイルCF(コンテンツプロバイダ作成)
ヘッダ部
コンテンツID
コンテンツデータ(商品)
(デジタル)署名データ(KCP,S)
ヘッダ
106
コンテンツ鍵データKc
権利書データ
コンテンツプロバイダ作成
暗号化
配信用鍵データKD1～KD6
キー(鍵)ファイルKF(EMDサービスセンター作成)
ヘッダ部
コンテンツID
コンテンツ鍵データKc+権利書データ
署名データ(KESC,S)
ヘッダデータ

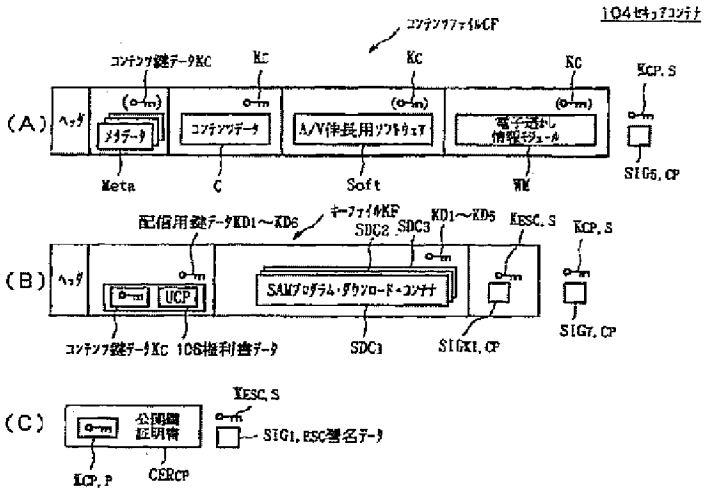
【図３】


101コンテンツプロバイダ
123
S115
116
改竄検査部
伸長部
112
S111
S112
113
S113
114
111
コンテンツマスターソースデータベース
電子透かし情報付加部
圧縮部
暗号化部(Kc)
Kc
C, Meta, Soft, WM
115
乱数発生部
118
124
セキュアコンテナ作成部
SAM管理部(通信ゲートウェイ)
KP
CERCP
SIG1,ESC
119
記憶部(データベース)
118b
118a
104セキュアコンテナ
104
Meta, Soft, WM
CERCP, SIG1, ESC
コンテンツID生成部
850
120
121
相互認証部
暗号化・復号部(Kss)
Kss
117
署名処理部(KCP,S)
122
権利管データ作成部
125
EMDサービスセンタ管理部(通信ゲートウェイ)

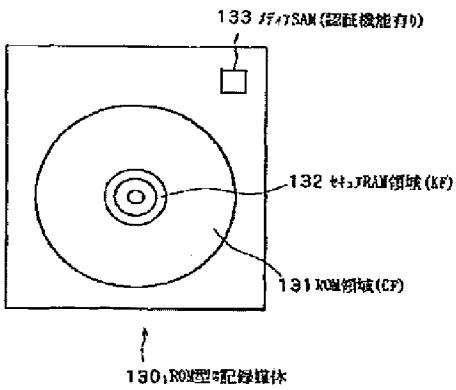
【図４】



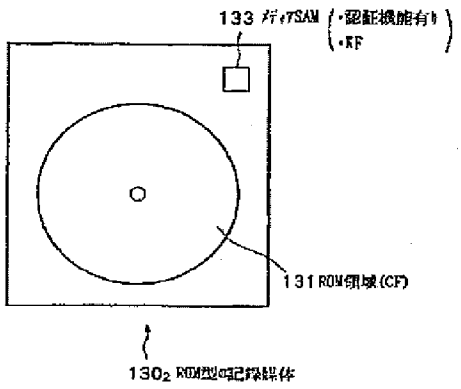
【図５】



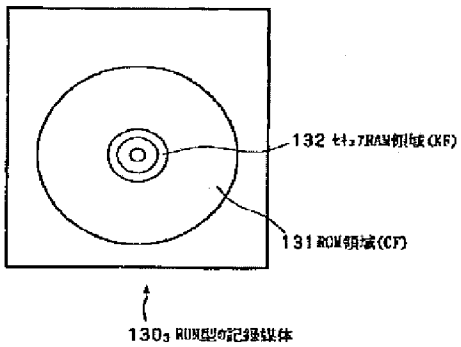
【図１２】



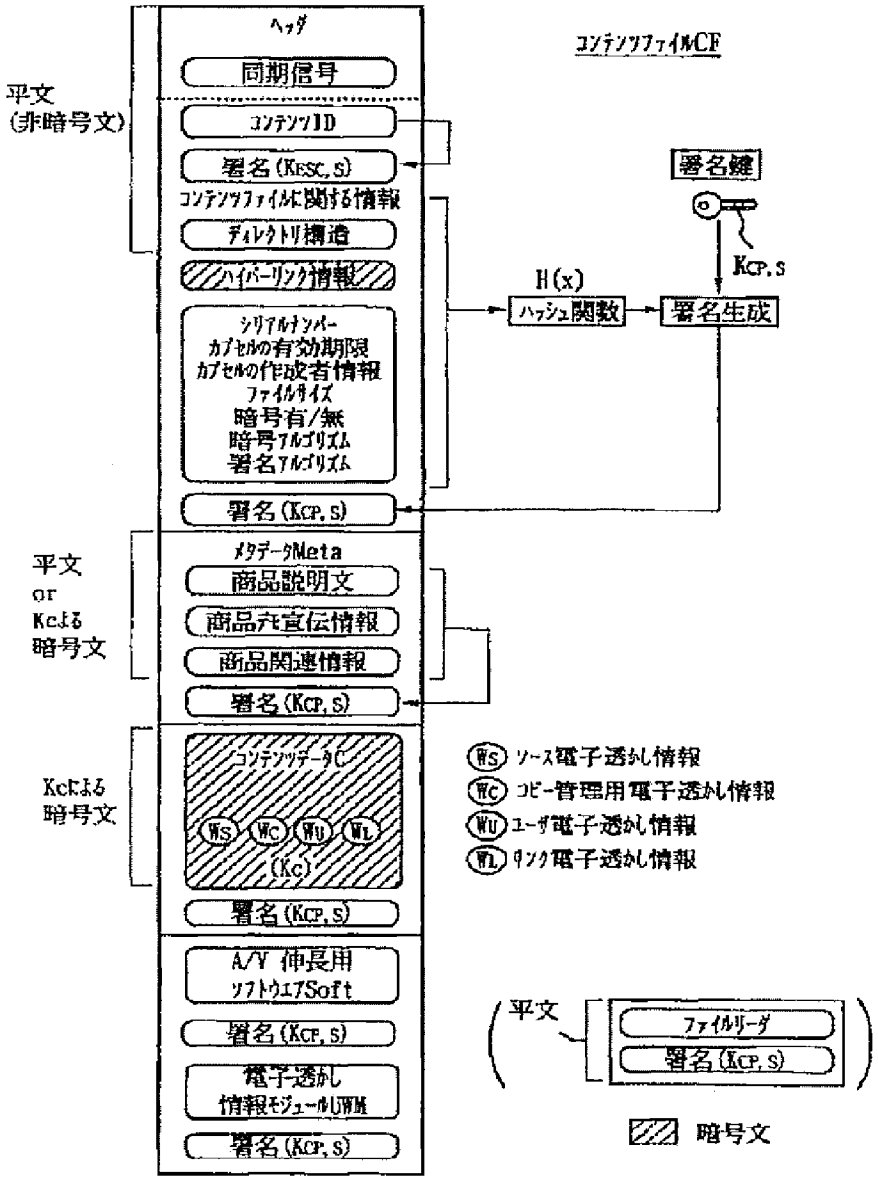
【図１３】



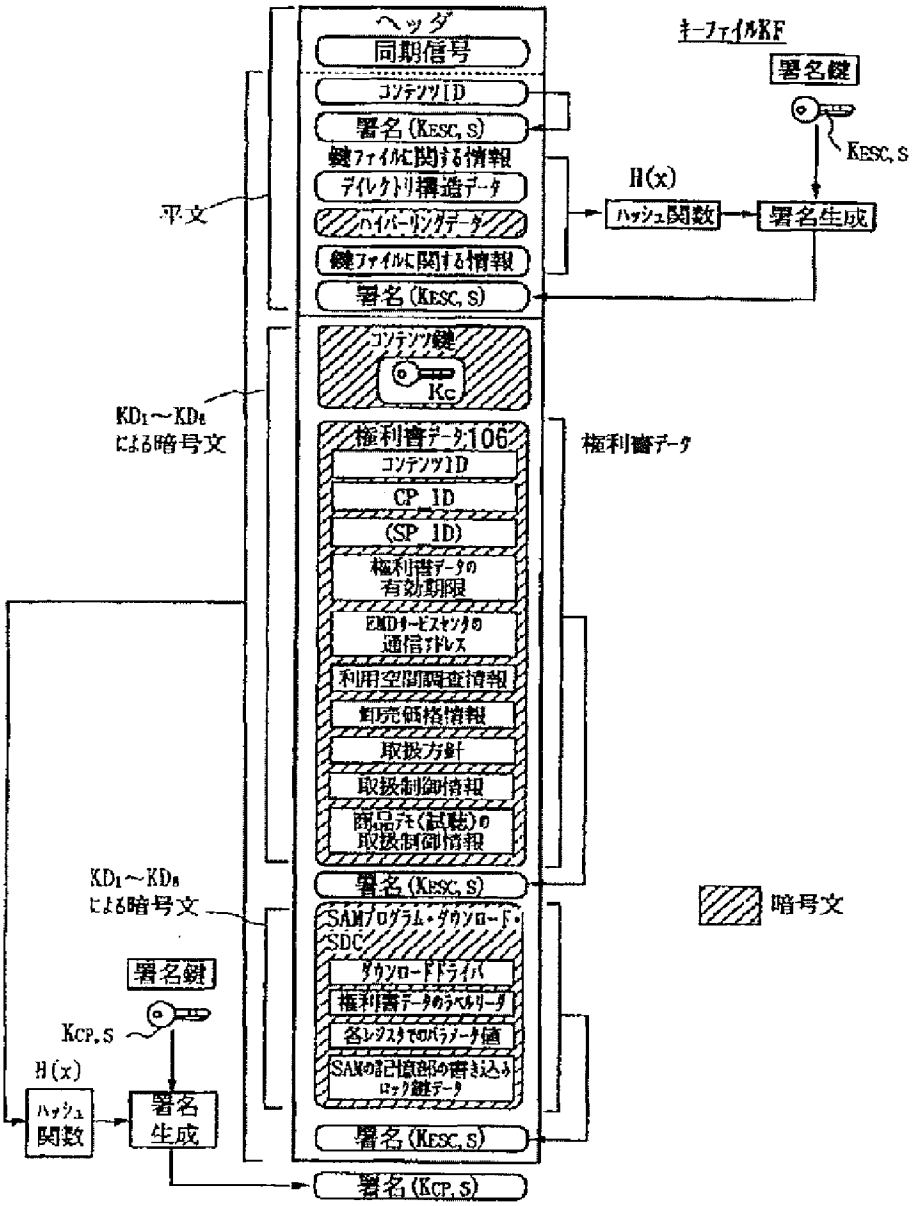
【図１４】



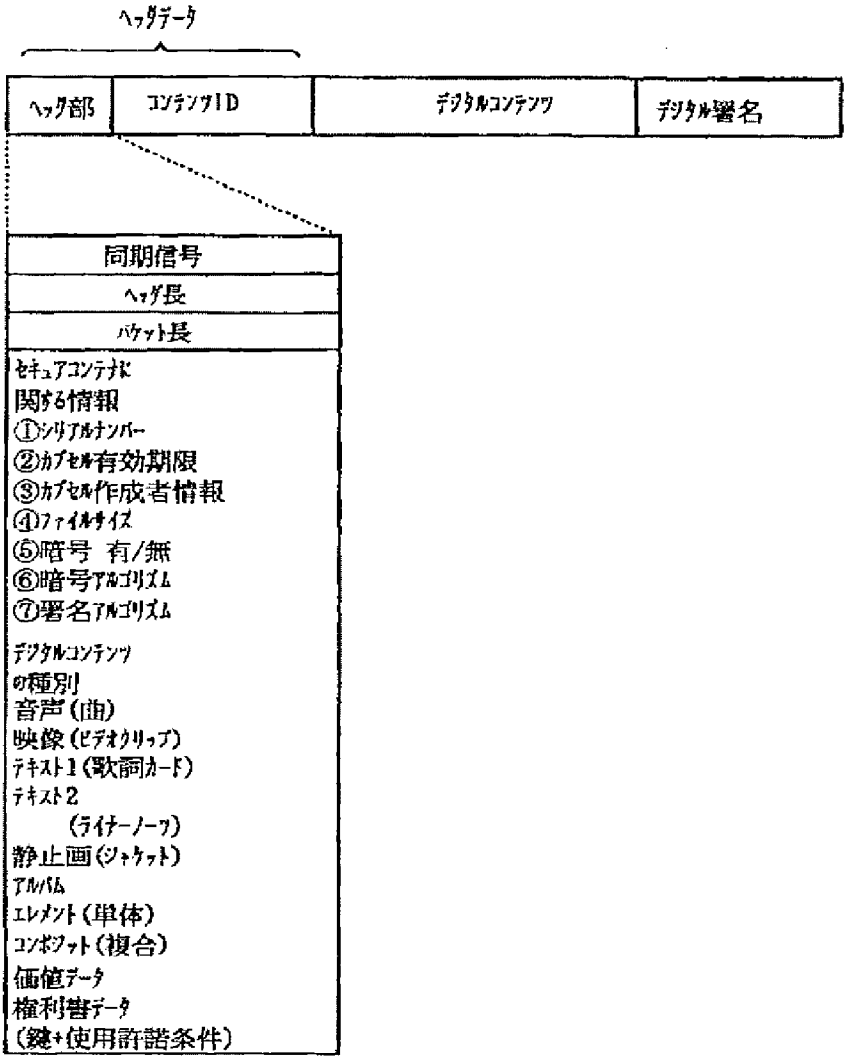
【図６】


ヘッダ
コンテンツファイルCF
同期信号
平文
(非暗号文)
コンテンツID
署名(KESC, S)
署名鍵
コンテンツファイルに関する情報
ディレクトリ構造
ハイパーリンク情報
H(x)
KCP, S
ハッシュ関数
署名生成
シリアルナンバー
カプセルの有効期限
カプセルの作成者情報
ファイルサイズ
暗号有/無
暗号アルゴリズム
署名アルゴリズム
署名(KCP, S)
メタデータMeta
平文
or
Kcよる
暗号文
商品説明文
商品売宣伝情報
商品関連情報
署名(KCP, S)
Kcによる
暗号文
コンテンツデータC
WS
WC
WU
WL
(Kc)
署名(KCP, S)
WS ソース電子透かし情報
WC コピー管理用電子透かし情報
WU ユーザ電子透かし情報
WL リンク電子透かし情報
A/V 伸長用
ソフトウエアSoft
署名(KCP, S)
電子透かし
情報モジュールUWM
署名(KCP, S)
平文
ファイルリーダ
署名(KCP, S)
暗号文

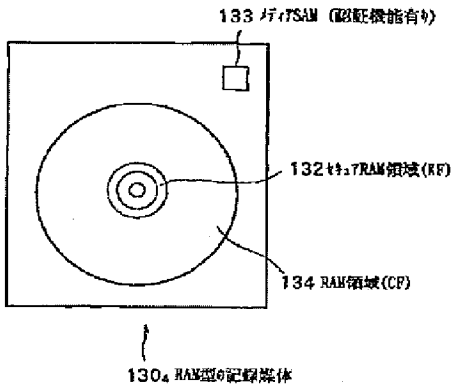
【図７】


ヘッダ
同期信号
コンテンツID
署名(KESC, S)
鍵ファイルに関する情報
ディレクトリ構造データ
ハイパーリンクデータ
鍵ファイルに関する情報
署名(KESC, S)
コンテンツ鍵
KC
権利書データ106
コンテンツID
CP_ID
(SP_ID)
権利書データの有効期限
EMDサービスセンタの通信アドレス
利用空間調査情報
卸売価格情報
取扱方針
取扱制御情報
商品デモ(試聴)の取扱制御情報
署名(KESC, S)
SAMプログラム・ダウンロード・SDC
ダウンロードドライバ
権利書データのラベルリード
各レジスタでのパラメータ値
SAMの記憶領部の書き込みロック鍵データ
署名(KESC, S)
署名(KCP, S)
平文
KD1～KD8による暗号文
KD1～KD8による暗号文
権利書データ
暗号文
キーファイルKF
署名鍵
KESC, S
H(x)
ハッシュ関数
署名生成
署名鍵
KCP, S
H(x)
ハッシュ関数
署名生成

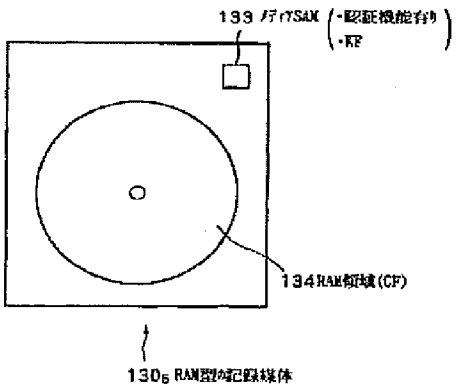
【図８】


ヘッダデータ
ヘッダ部
コンテンツID
デジタルコンテンツ
デジタル署名
同期信号
ヘッダ長
パケット長
セキュアコンテナに
関する情報
①シリアルナンバー
②カプセル有効期限
③カプセル作成者情報
④ファイルサイズ
⑤暗号 有/無
⑥暗号アルゴリズム
⑦署名アルゴリズム
デジタルコンテンツ
の種別
音声(曲)
映像(ビデオクリップ)
テキスト1(歌詞カード)
テキスト2
(ライナーノーツ)
静止画(ジャケット)
アルバム
エレメント(単体)
コンポジット(複合)
価値データ
権利書データ
(鍵+使用許諾条件)

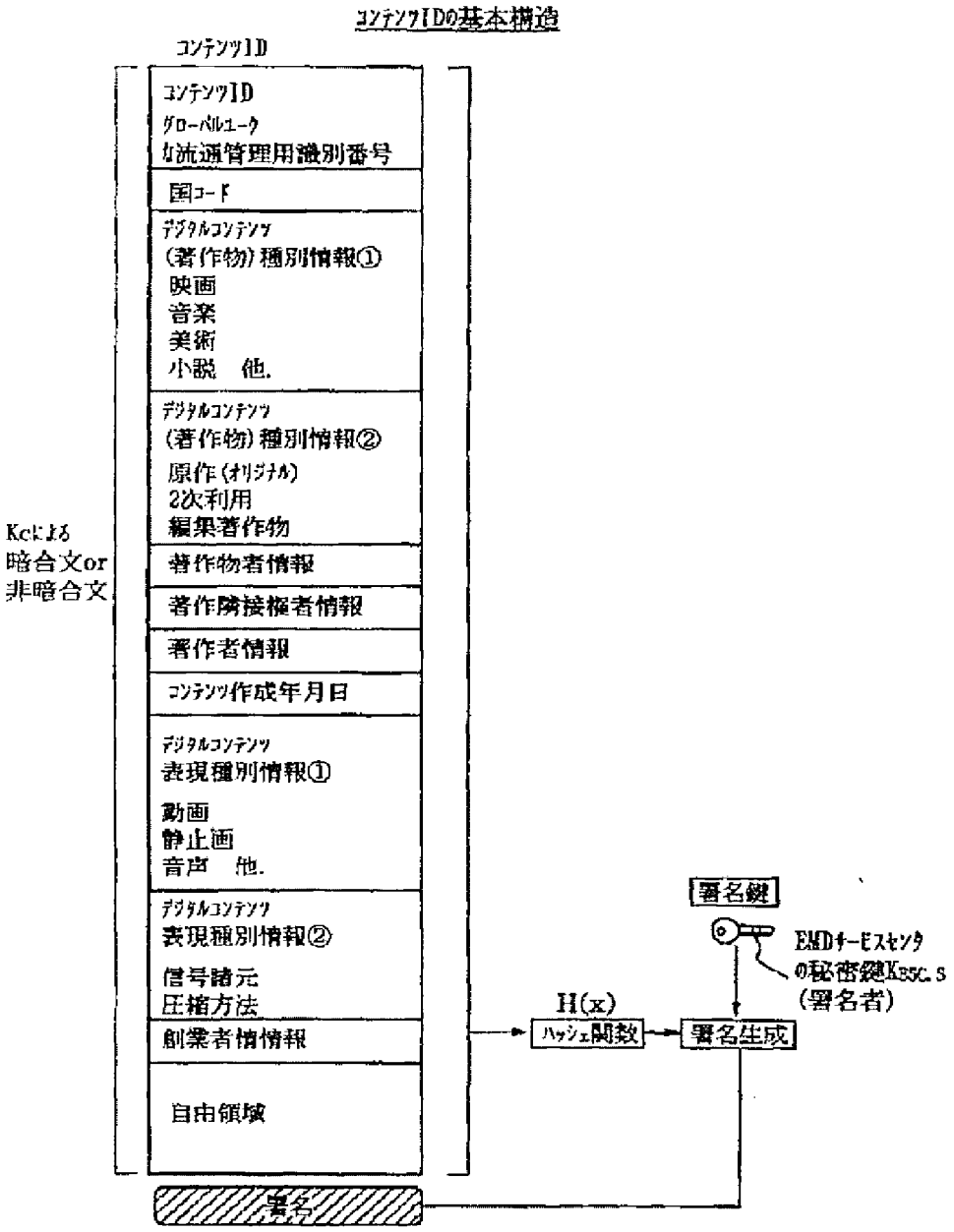
【図１５】


133 メディアSAM (認証機能有り)
132 セキュアRAM領域(KF)
134 RAM領域(CF)
130₄ RAM型の記録媒体

【図１６】

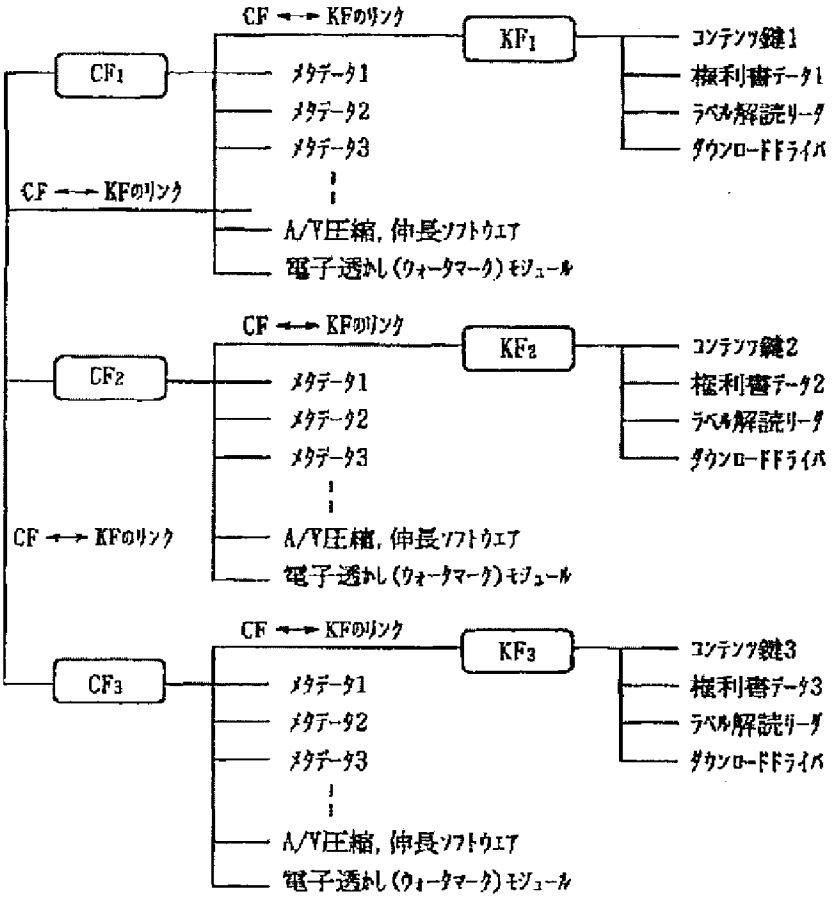

133 メディアSAM (-認証機能有り -KF)
134 RAM領域(CF)
130₅ RAM型の記録媒体

【図９】

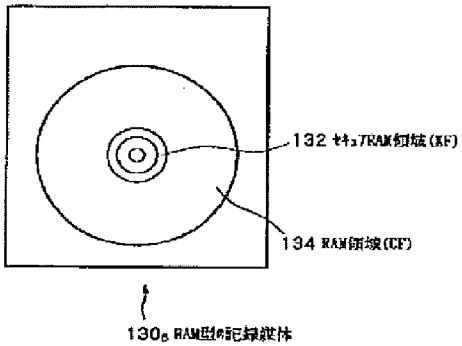

コンテンツIDの基本構造
コンテンツID
コンテンツID
グローバルユーク
u流通管理用識別番号
国コード
デジタルコンテンツ
(著作物)種別情報①
映画
音楽
美術
小説　他.
デジタルコンテンツ
(著作物)種別情報②
原作(オリジナル)
2次利用
編集著作物
著作物者情報
著作隣接権者情報
著作者情報
コンテンツ作成年月日
デジタルコンテンツ
表現種別情報①
動画
静止画
音声　他.
デジタルコンテンツ
表現種別情報②
信号諸元
圧縮方法
創業者情情報
自由領域
Kcによる
暗合文or
非暗合文
署名
H(x)
ハッシュ関数
署名生成
署名鍵
EMDサービスセンタ
の秘密鍵Kesc.s
(署名者)

【図１０】

セキュアコンテナのディレクトリ構造



【図１７】

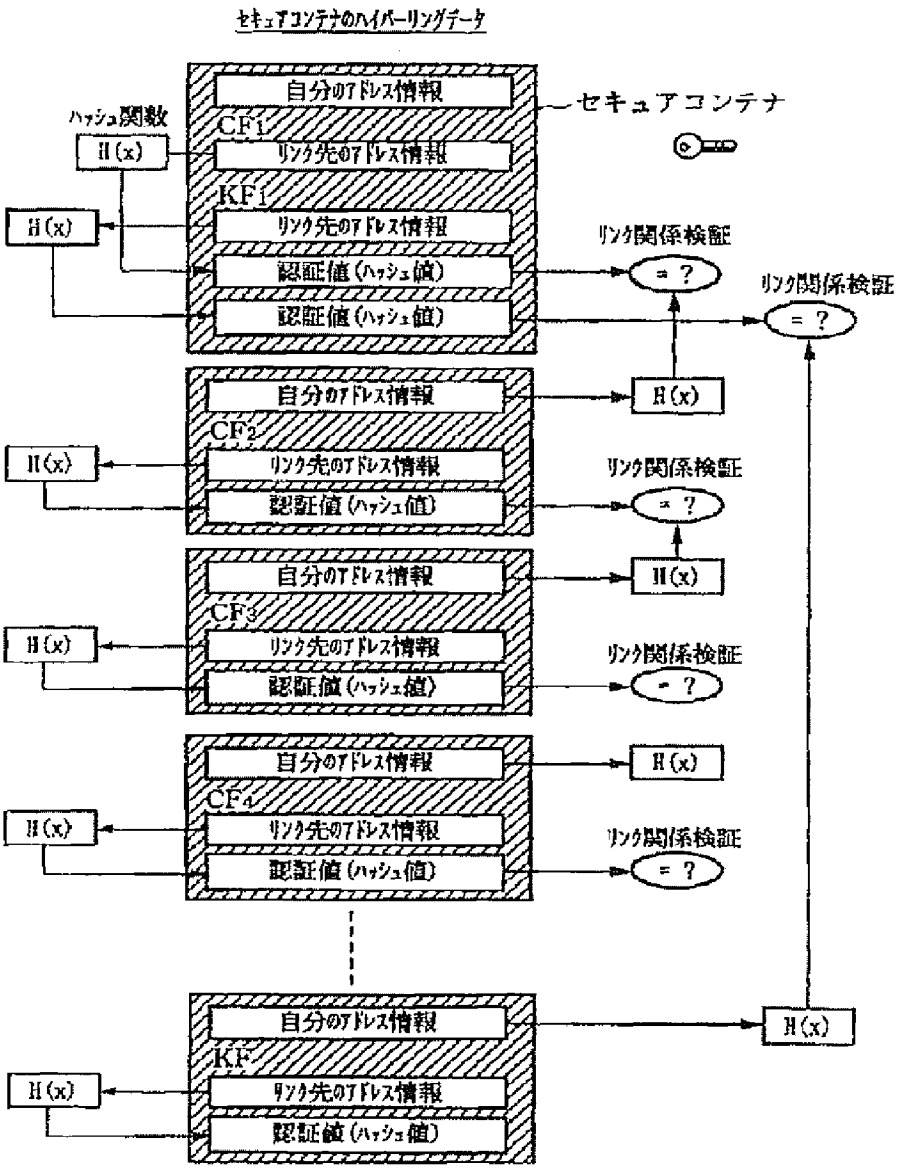


【図２８】

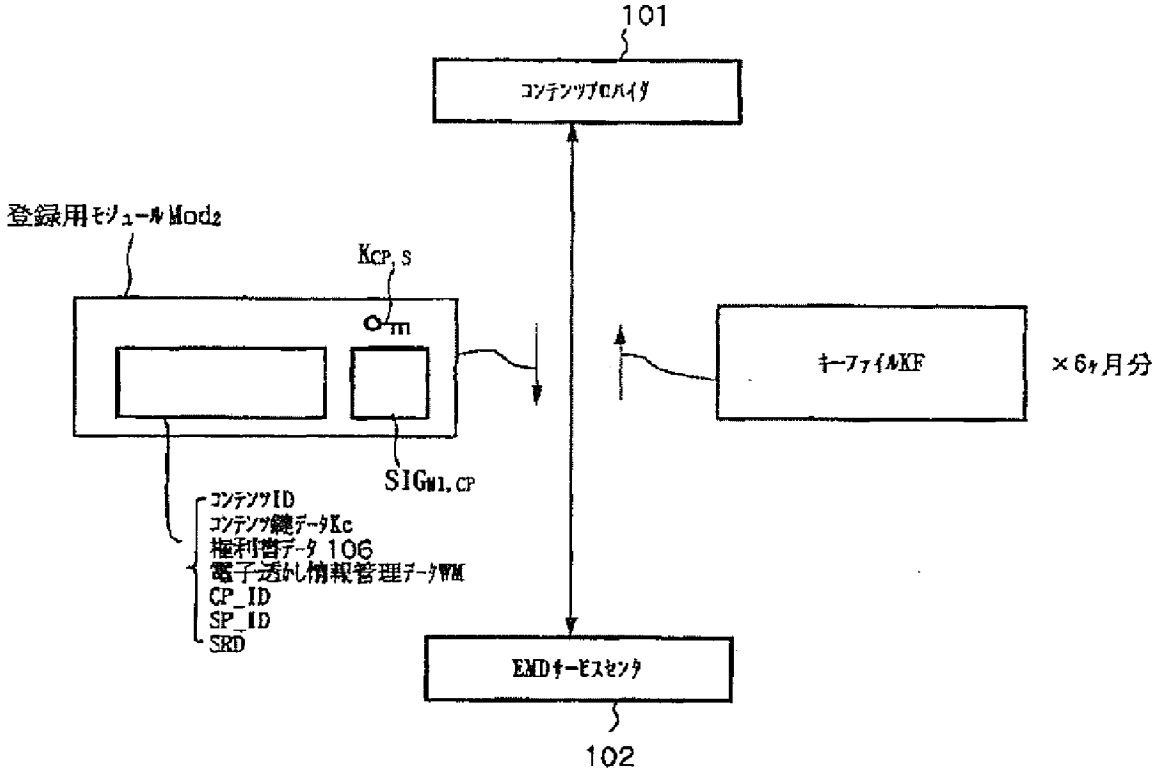
スタックメモリ200に記憶されるデータ

コンテンツ鍵データKc
権利書データ（UCP）106
記憶部3（フラッシュメモリ）192のロック鍵データK_{LOC}
コンテンツプロバイダ101の公開鍵証明書CER_{CP}
利用制御情状態データ（UCS）166
SAMプログラム・ダウンロード・コンテナSD_1～SDC_3

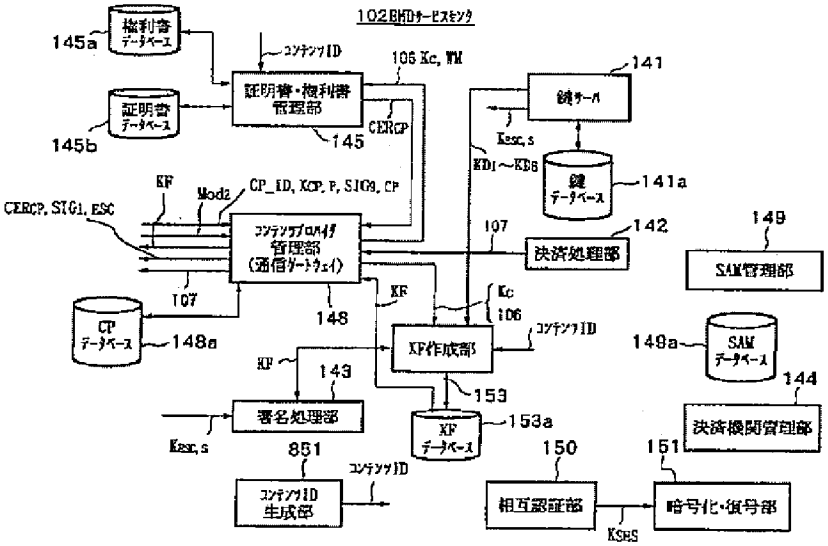
【図１１】


セキュアコンテナのハイパーリングデータ
セキュアコンテナ
ハッシュ関数
H(x)
CF1
自分のアドレス情報
リンク先のアドレス情報
KF1
リンク先のアドレス情報
認証値(ハッシュ値)
認証値(ハッシュ値)
リンク関係検証
= ?
リンク関係検証
= ?
CF2
自分のアドレス情報
リンク先のアドレス情報
認証値(ハッシュ値)
CF3
自分のアドレス情報
リンク先のアドレス情報
認証値(ハッシュ値)
CF4
自分のアドレス情報
リンク先のアドレス情報
認証値(ハッシュ値)
KF
自分のアドレス情報
リンク先のアドレス情報
認証値(ハッシュ値)

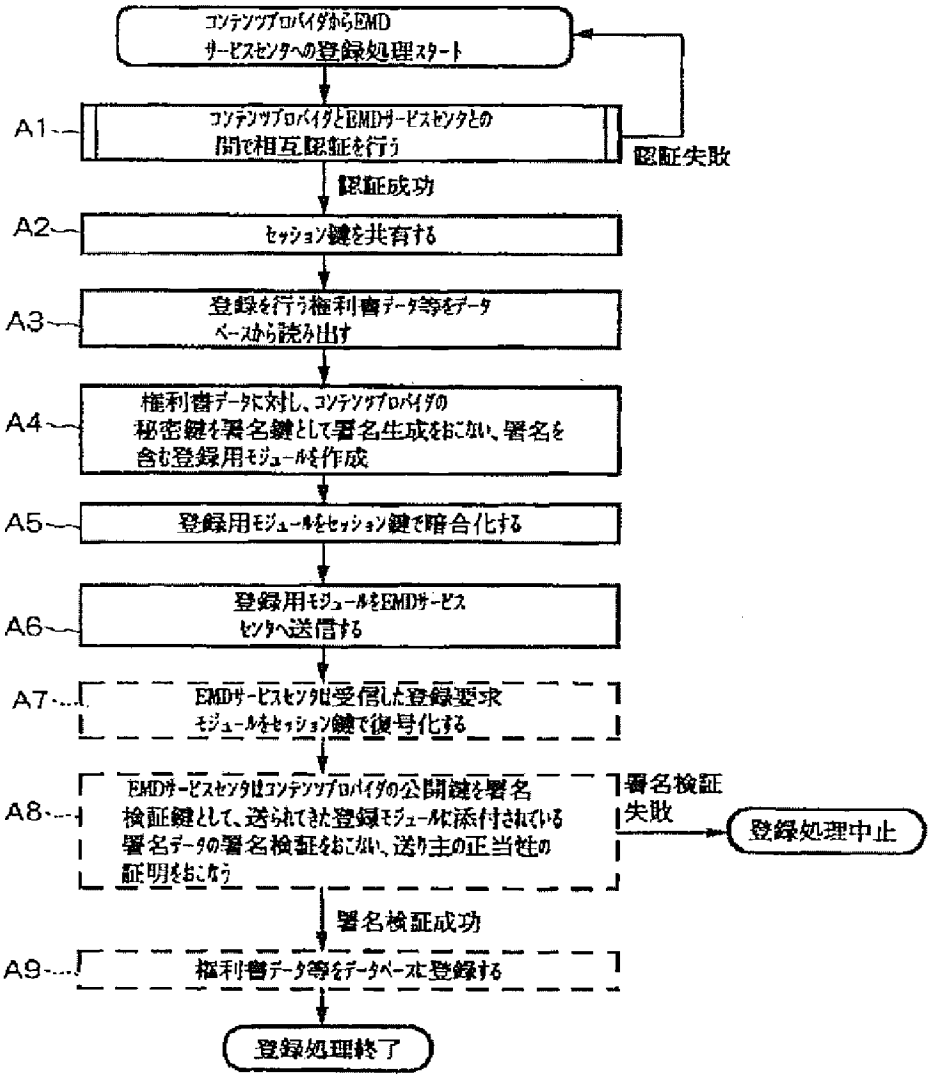
【図１８】


101
コンテンツプロバイダ
登録用モジュールMod2
Kcp, s
キーファイルKF
×6ヶ月分
SIGw1, CP
コンテンツID
コンテンツ鍵データKc
権利書データ106
電子透かし情報管理データWM
CP_ID
SP_ID
SRD
EMDサービスセンタ
102

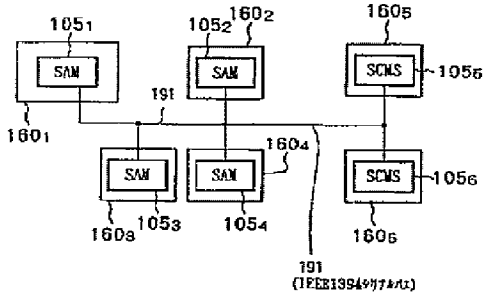
【図２３】


102 EMDサービスセンタ
145a
権利書データベース
コンテンツID
105 Kc, WM
141
証明書・権利書管理部
鍵サーバ
145b
証明書データベース
CERCP
145
Kesc, s
KD1～KD6
鍵データベース
141a
KF
Mod2
CP_ID, KCP, P, SIG3, CP
CERCP, SIG1, ESC
コンテンツプロバイダ管理部（通信ゲートウェイ）
107
142
決済処理部
149
SAM管理部
107
148
KF
Kc
106
CPデータベース
148a
KF作成部
コンテンツID
149a
SAMデータベース
144
KF
143
153
署名処理部
KF データベース
153a
決済機関管理部
Kesc, s
851
150
151
コンテンツID
コンテンツID生成部
相互認証部
暗号化・復号部
KSES

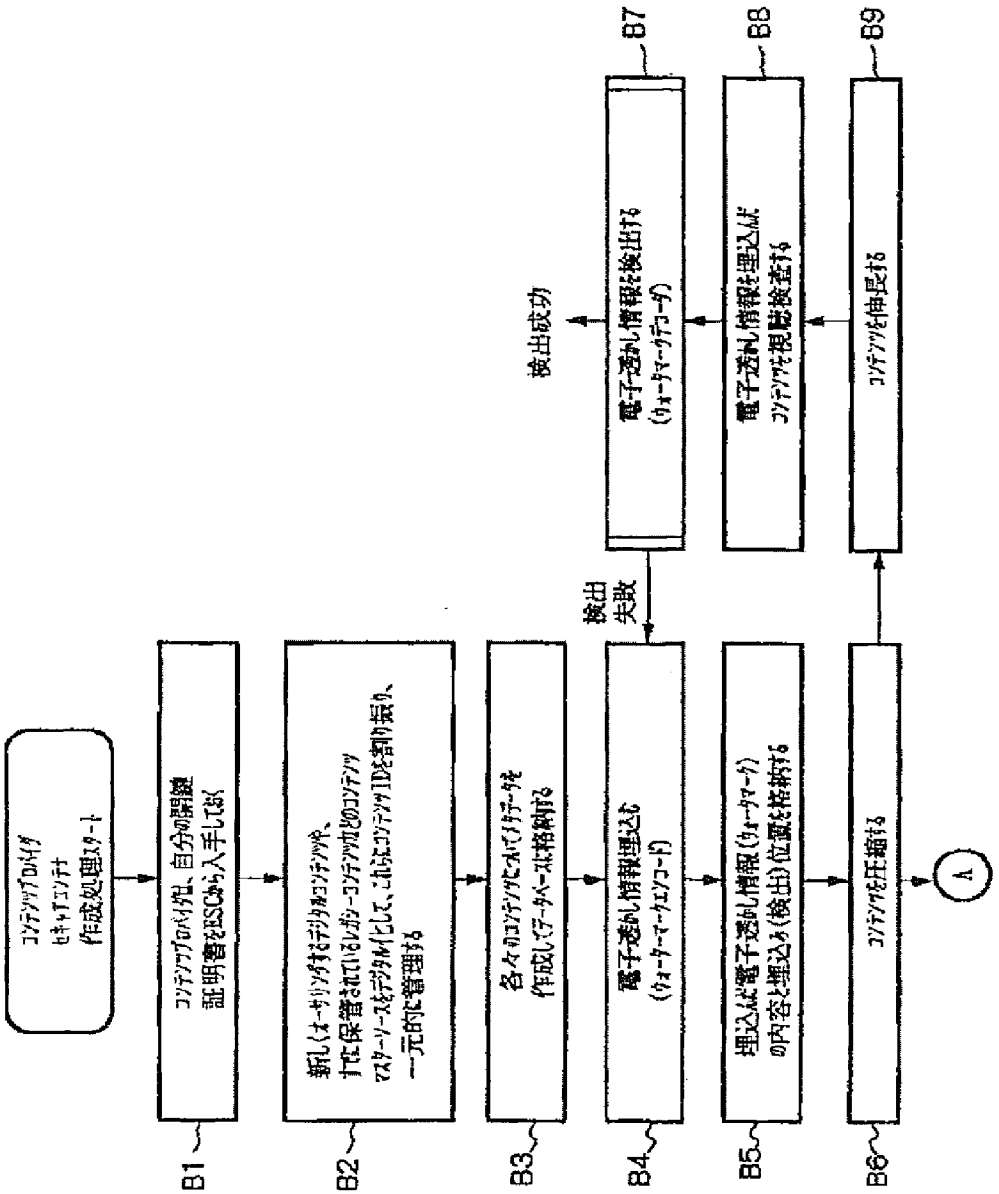
【図１９】


コンテンツプロバイダからEMD
サービスセンタへの登録処理スタート
A1
コンテンツプロバイダとEMDサービスセンタとの
間で相互認証を行う
認証失敗
認証成功
A2
セッション鍵を共有する
A3
登録を行う権利書データ等をデータ
ベースから読み出す
A4
権利書データに対し、コンテンツプロバイダの
秘密鍵を署名鍵として署名生成をおこない、署名を
含む登録用モジュールを作成
A5
登録用モジュールをセッション鍵で暗合化する
A6
登録用モジュールをEMDサービス
センタへ送信する
A7
EMDサービスセンタは受信した登録要求
モジュールをセッション鍵で復号化する
A8
EMDサービスセンタはコンテンツプロバイダの公開鍵を署名
検証鍵として、送られてきた登録モジュールに添付されている
署名データの署名検証をおこない、送り主の正当性の
証明をおこなう
署名検証
失敗
登録処理中止
署名検証成功
A9
権利書データ等をデータベースに登録する
登録処理終了

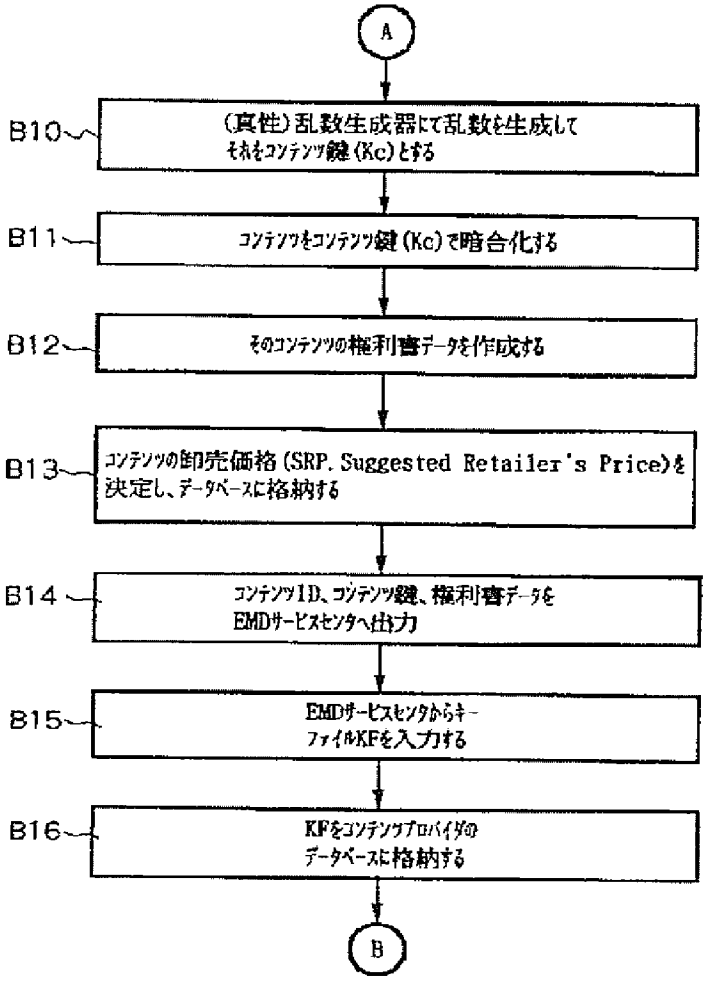
【図４４】


1051
1052
1602
1605
SAM
SAM
SCMS
1055
191
1601
SAM
SAM
1604
SCMS
1056
1603
1053
1054
1606
191
(IEEE1394ケーブル)

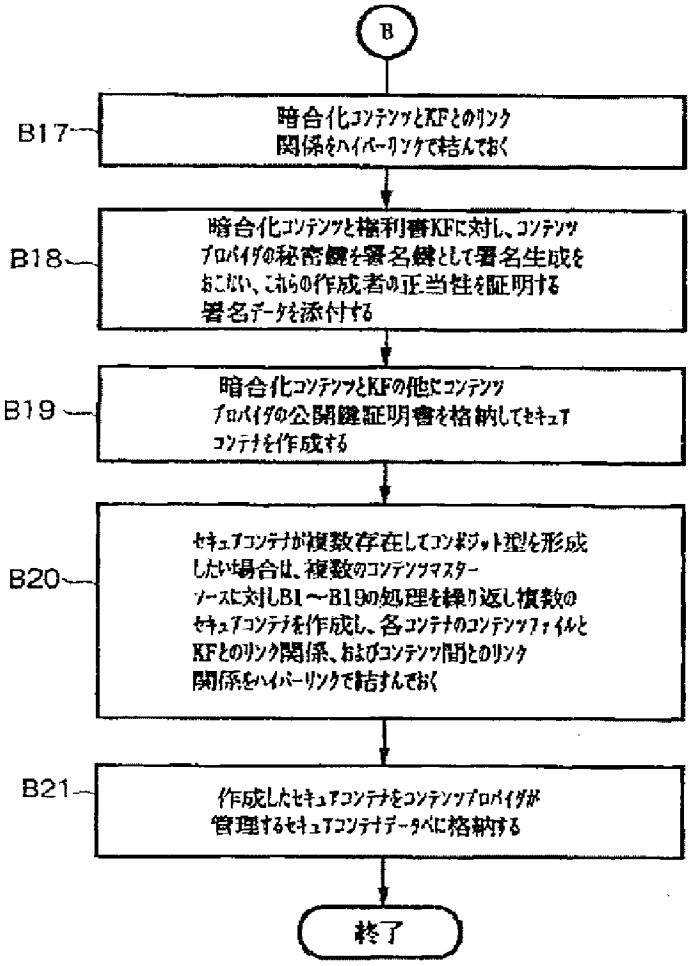
【図２０】



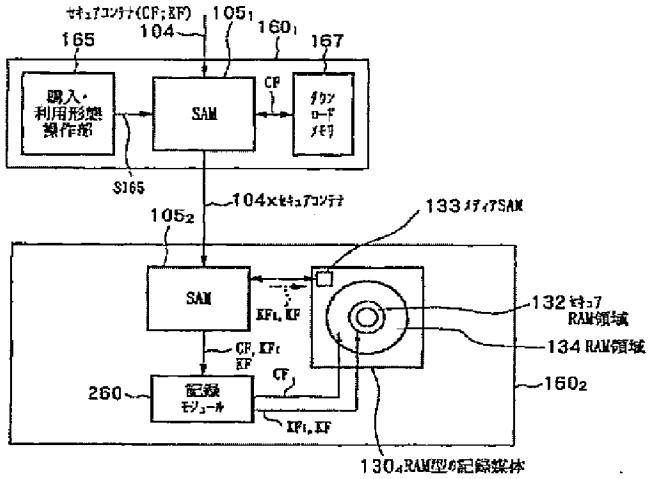
【図２１】


A
B10
(真性)乱数生成器にて乱数を生成して
それをコンテンツ鍵(Kc)とする
B11
コンテンツをコンテンツ鍵(Kc)で暗合化する
B12
そのコンテンツの権利書データを作成する
B13
コンテンツの卸売価格(SRP. Suggested Retailer's Price)を
決定し、データベースに格納する
B14
コンテンツID、コンテンツ鍵、権利書データを
EMDサービスセンタへ出力
B15
EMDサービスセンタからキー
ファイルKFを入力する
B16
KFをコンテンツプロバイダの
データベースに格納する
B

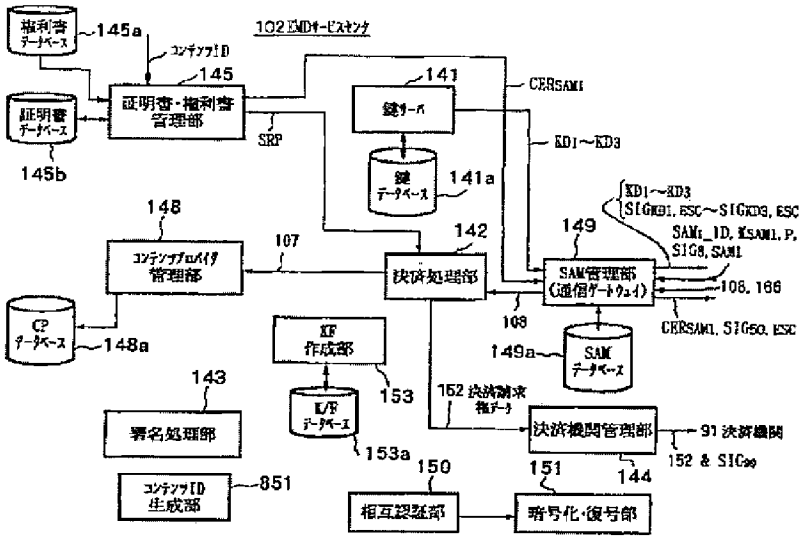
【図２２】


B
B17
暗合化コンテンツとKFとのリンク
関係をハイパーリンクで結んでおく
B18
暗合化コンテンツと権利書KFに対し、コンテンツ
プロバイダの秘密鍵を署名鍵として署名生成を
おこない、これらの作成者の正当性を証明する
署名データを添付する
B19
暗合化コンテンツとKFの他にコンテンツ
プロバイダの公開鍵証明書を格納してセキュア
コンテナを作成する
B20
セキュアコンテナが複数存在してコンポジット型を形成
したい場合は、複数のコンテンツマスター
ソースに対しB1～B19の処理を繰り返し複数の
セキュアコンテナを作成し、各コンテナのコンテンツファイルと
KFとのリンク関係、およびコンテンツ間とのリンク
関係をハイパーリンクで結んでおく
B21
作成したセキュアコンテナをコンテンツプロバイダが
管理するセキュアコンテナデータベに格納する
終了

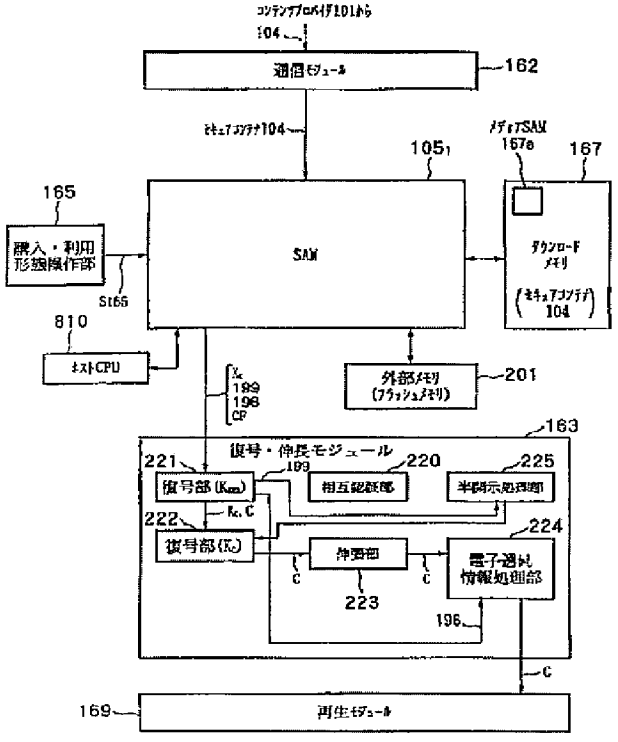
【図３２】


セキュアコンテナ(CF;KF)
105₁
165
104
160₁
167
購入・
利用形態
操作部
SAM
CF
ダウン
ロード
メモリ
S165
104×セキュアコンテナ
105₂
133 メディアSAM
SAM
KF₁, KF
132 セキュア
RAM領域
134 RAM領域
CF, KF₂
KF
CF
260
記録
モジュール
160₂
KF₁, KF
130 RAM型の記録媒体

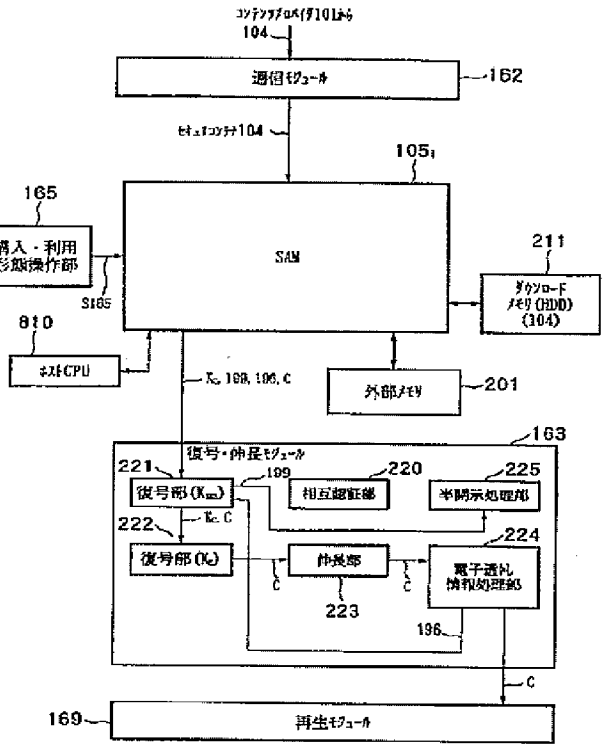
【図２４】


権利書データベース
145a
コンテンツID
145
証明書・権利書管理部
証明書データベース
145b
SRP
141
鍵サーバ
CERSAM1
KD1～KD3
鍵データベース
141a
148
コンテンツプロバイダ管理部
107
142
決済処理部
149
SAM管理部（通信ゲートウェイ）
KD1～KD3
SIGKD1, ESC～SIGKD3, ESC
SAM1_ID, KSAM1, P, SIG8, SAM1
108, 166
CERSAM1, SIG50, ESC
CP データベース
148a
108
149a
SAM データベース
KF 作成部
153
K/F データベース
153a
143
署名処理部
152 決済請求指データ
決済機関管理部
91 決済機関
152 & SIG99
151
144
コンテンツID生成部
851
150
相互認証部
暗号化・復号部

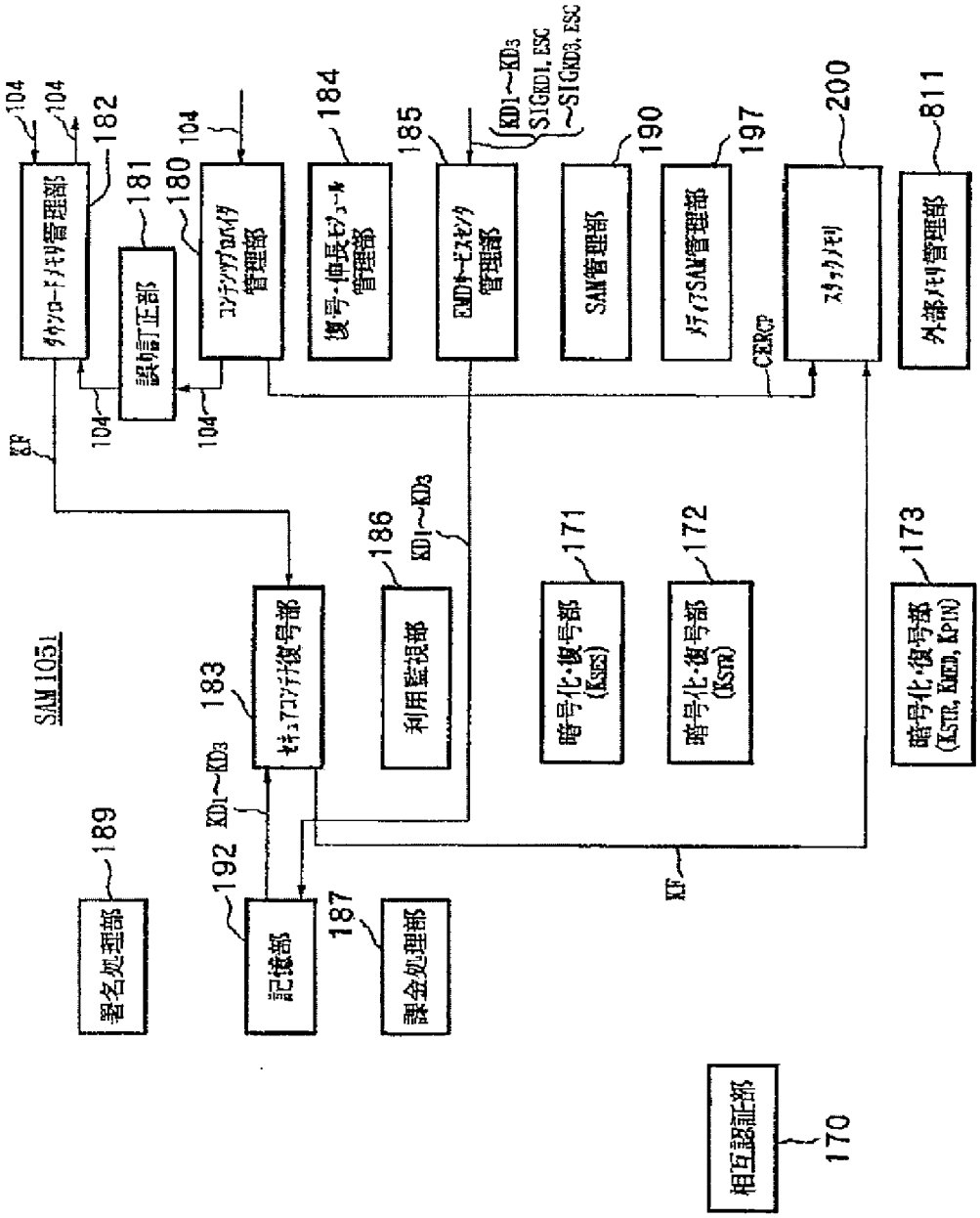
【図２５】


コンテンツプロバイダ101から
104
通信モジュール
162
セキュアコンテナ104
メディアSAM
167a
167
105₁
165
購入・利用形態操作部
SAM
ダウンロードメモリ
（セキュアコンテナ104）
St65
810
ホストCPU
Kc, 198, CP
外部メモリ（フラッシュメモリ）
201
163
復号・伸長モジュール
221
復号部（Kcm）
199
220
相互認証部
225
半開示処理部
222
復号部（Kc）
Kc, C
224
伸長部
電子透かし情報処理部
223
196
C
169
再生モジュール

【図２９】

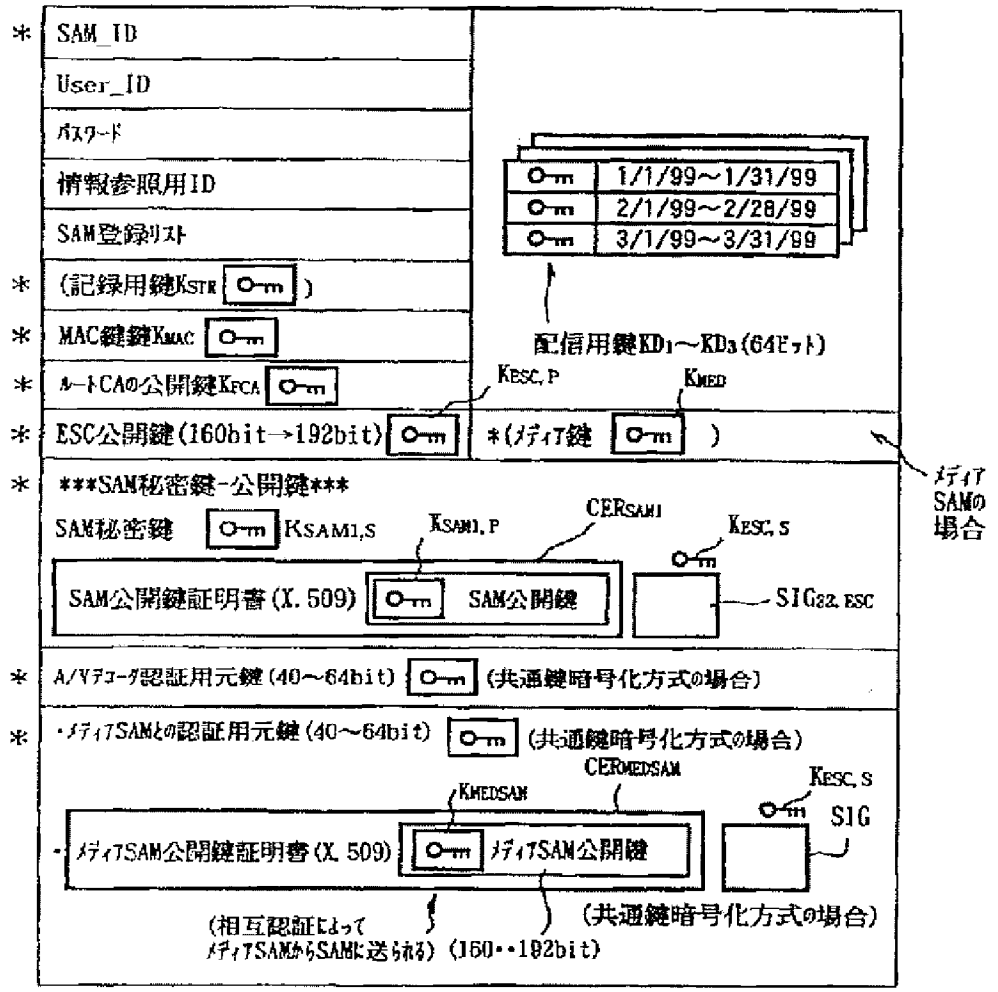

コンテンツプロバイダ101から
104
通信モジュール
162
セキュアコンテナ104
105₁
165
購入・利用形態操作部
SAM
211
ダウンロードメモリ（HDD）（104）
St65
810
ホストCPU
Kc, 198, 196, C
外部メモリ
201
163
復号・伸長モジュール
221
復号部（Kcm）
199
220
相互認証部
225
半開示処理部
222
復号部（Kc）
Kc, C
224
伸長部
電子透かし情報処理部
223
196
C
169
再生モジュール

【図２６】

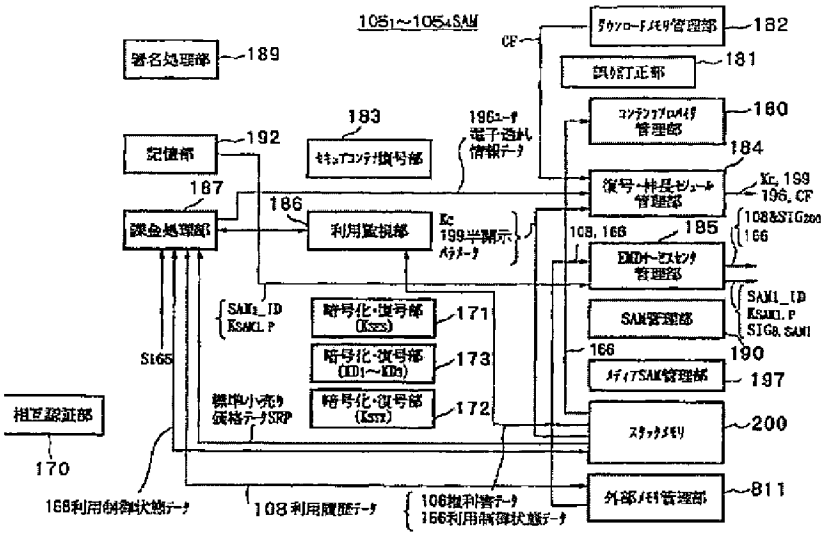

SAM 1051
104
182
181
180
184
185
190
197
200
811
KD1～KD3
SIGKD1, ESC
SIGKD3, ESC
CERCP
KF
186
171
172
173
183
192
187
189
170
署名処理部
記録部
課金処理部
相互認証部

【図３０】

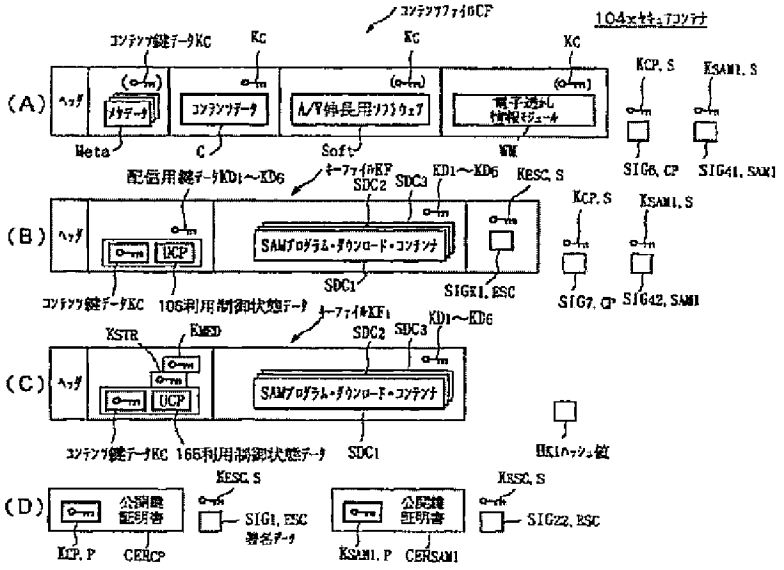
記憶部192に記憶されるデータ



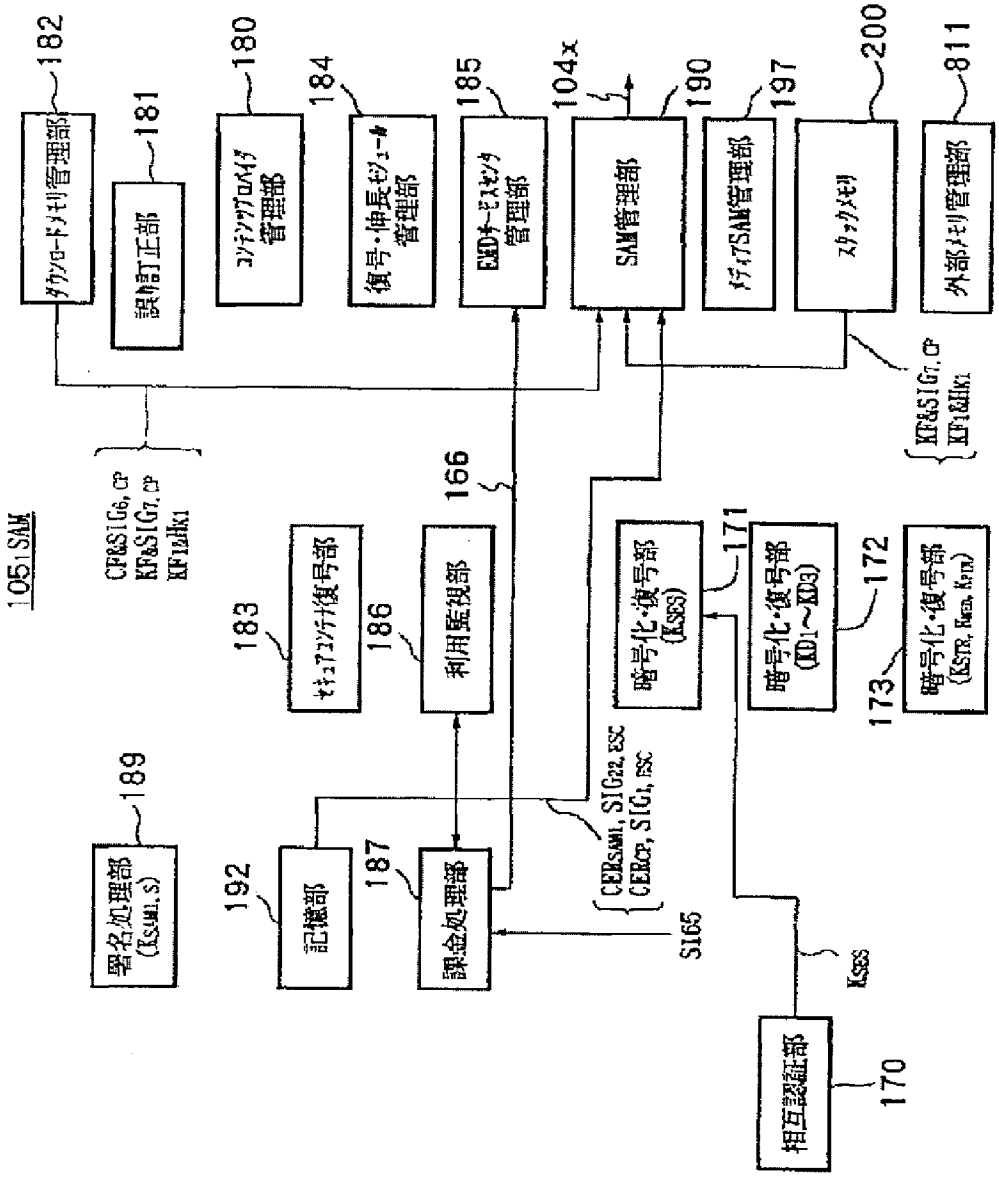
【図３１】


1051～1054SAM
署名処理部
189
記憶部
192
183
セキュアコンテナ復号部
196ユーザ電子透かし情報データ
187
課金処理部
186
利用監視部
Kc 199半導体パラメータ
CP
ダウンロードメモリ管理部
182
誤り訂正部
181
コンテンツプログラム管理部
180
184
復号・伸長モジュール管理部
Kc, 199 196, CF
108&SIG200 166
108, 166
185
EMDサービスセンタ管理部
SAM1_ID KSAM1, P SIG8, SAM1
SAM管理部
166
190
メディアSAM管理部
197
スタックメモリ
200
外部メモリ管理部
811
SAMx_ID KSAMx, P
暗号化・復号部 (KSES)
171
暗号化・復号部 (KD1～KD6)
173
暗号化・復号部 (KSTR)
172
S165
標準小売り価格データSRP
相互認証部
170
168利用制御状態データ
108利用履歴データ
106権利書データ 166利用制御状態データ

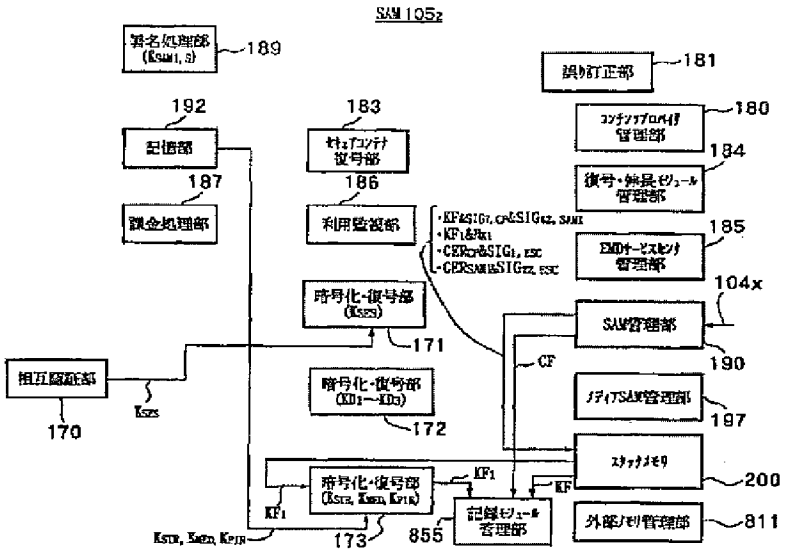
【図３４】


コンテンツファイルCF
104セキュアコンテナ
コンテンツ鍵データKC
Kc
Kc
Kc
(A)
ヘッダ
メタデータ
コンテンツデータ
ムペア特長用ソフトウェア
電子透かし情報モジュール
Meta
C
Soft
WM
KCP, S
KSAM1, S
SIG6, CP
SIG41, SAM1
配信用鍵データKD1～KD6
キーファイルKF
SDC2
SDC3
KD1～KD6
KESC, S
(B)
UCP
SAMプログラム・ダウンロード・コンテンツ
SDC1
SIG81, ESC
KCP, S
KSAM1, S
SIG7, CP
SIG42, SAM1
コンテンツ鍵データKC
106利用制御状態データ
KSTR
KMED
(C)
165利用制御状態データ
HK1ハッシュ値
(D)
公開鍵証明書
KESC, S
SIG1, ESC
署名データ
KCP, P
CERCP
KSAM1, P
CERSAM1
SIG22, ESC

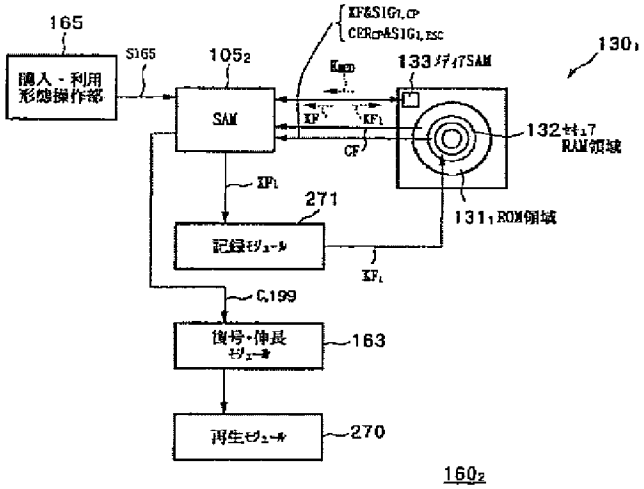
【図３３】


105₁ SAM
182
ダウンロードメモリ管理部
181
誤制訂正部
180
コンテンツプロバイダ管理部
184
復号・伸長モジュール管理部
185
EMDサービスセンタ管理部
104x
SAM管理部
190
メディアSAM管理部
197
200
スタックメモリ
811
外部メモリ管理部
CP&SIG6, CP
KF&SIG7, CP
KF1&Hk1
KF&SIG7, CP
KF1&Hk1
166
183
セキュアコンテナ復号部
186
利用監視部
暗号化・復号部 (Kssss)
171
暗号化・復号部 (KD1～KD3)
172
173
暗号化・復号部 (Kstr, Kmta, Kmtb)
189
署名処理部 (Kcum1, s)
192
記憶部
187
課金処理部
CERsam1, SIG22, ESC
CERcp, SIG1, ESC
S165
Kssss
170
相互認証部

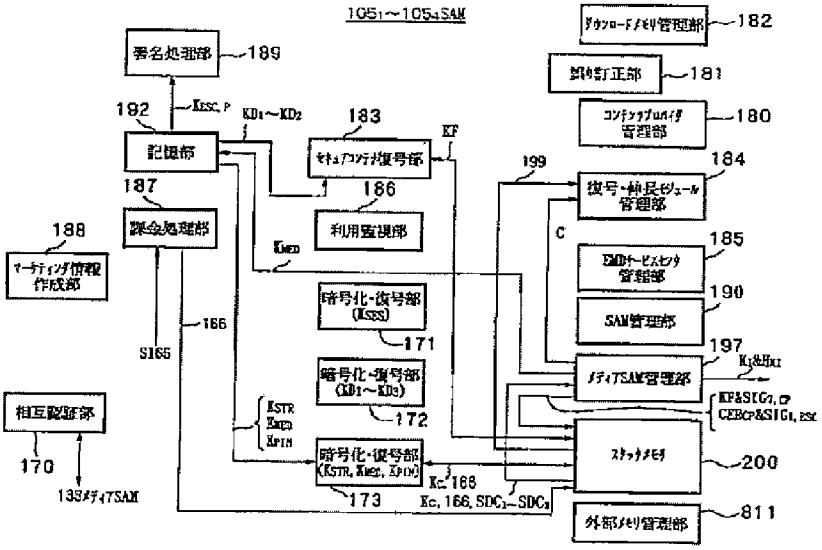
【図３５】


SAM 105₂
署名処理部
189
誤り訂正部
181
192
183
180
記憶部
コンテンツ復号部
コンテンツプロバイダ管理部
184
187
186
復号・伸長モジュール管理部
課金処理部
利用管理部
185
EMDサービスセンタ管理部
104x
暗号化・復号部
SAM管理部
171
190
相互認証部
CF
メディアSAM管理部
197
暗号化・復号部
172
ステップメモリ
200
暗号化・復号部
KF1
KF
KF1
記録モジュール管理部
855
外部メモリ管理部
811
173
170

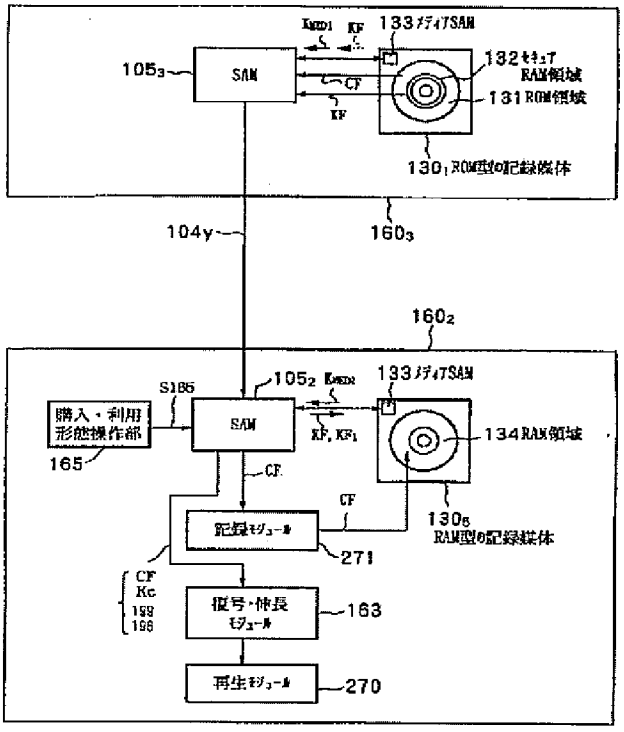
【図３６】


165
S165
105₂
133 メディアSAM
130₁
購入・利用形態操作部
SAM
132 セキュア RAM領域
271
131₁ ROM領域
C,199
復号・伸長モジュール
163
再生モジュール
270
160₂

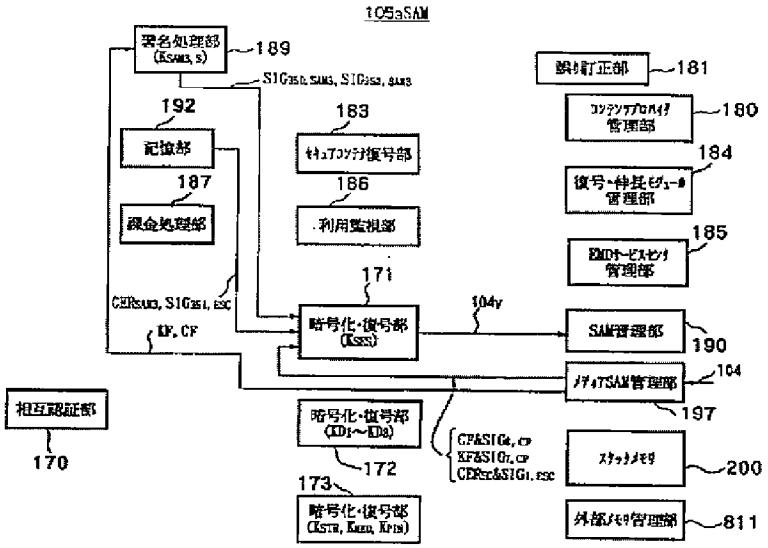
【図３７】


105₁～105₄SAM
署名処理部
189
182
記憶部
183
186
利用監視部
187
課金処理部
188
マーケティング情報作成部
166
S165
暗号化・復号部(KSES)
171
暗号化・復号部(KD1～KD3)
172
暗号化・復号部(KSTR, KMED, KPDG)
173
相互認証部
170
133メディアSAM
199
184
185
190
197
200
811
C
Kc, 166, SDC₁～SDC₃

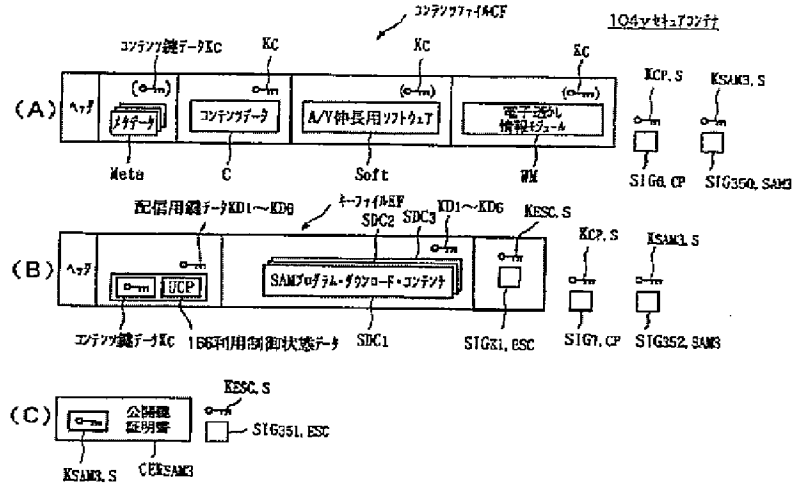
【図３８】


133メディアSAM
105₃
SAM
CF
132セキュアRAM領域
131 ROM領域
130₁ ROM型の記録媒体
104y
160₃
160₂
105₂
S165
購入・利用形態操作部
165
134 RAM領域
130₆ RAM型の記録媒体
記録モジュール
271
復号・伸長モジュール
163
再生モジュール
270

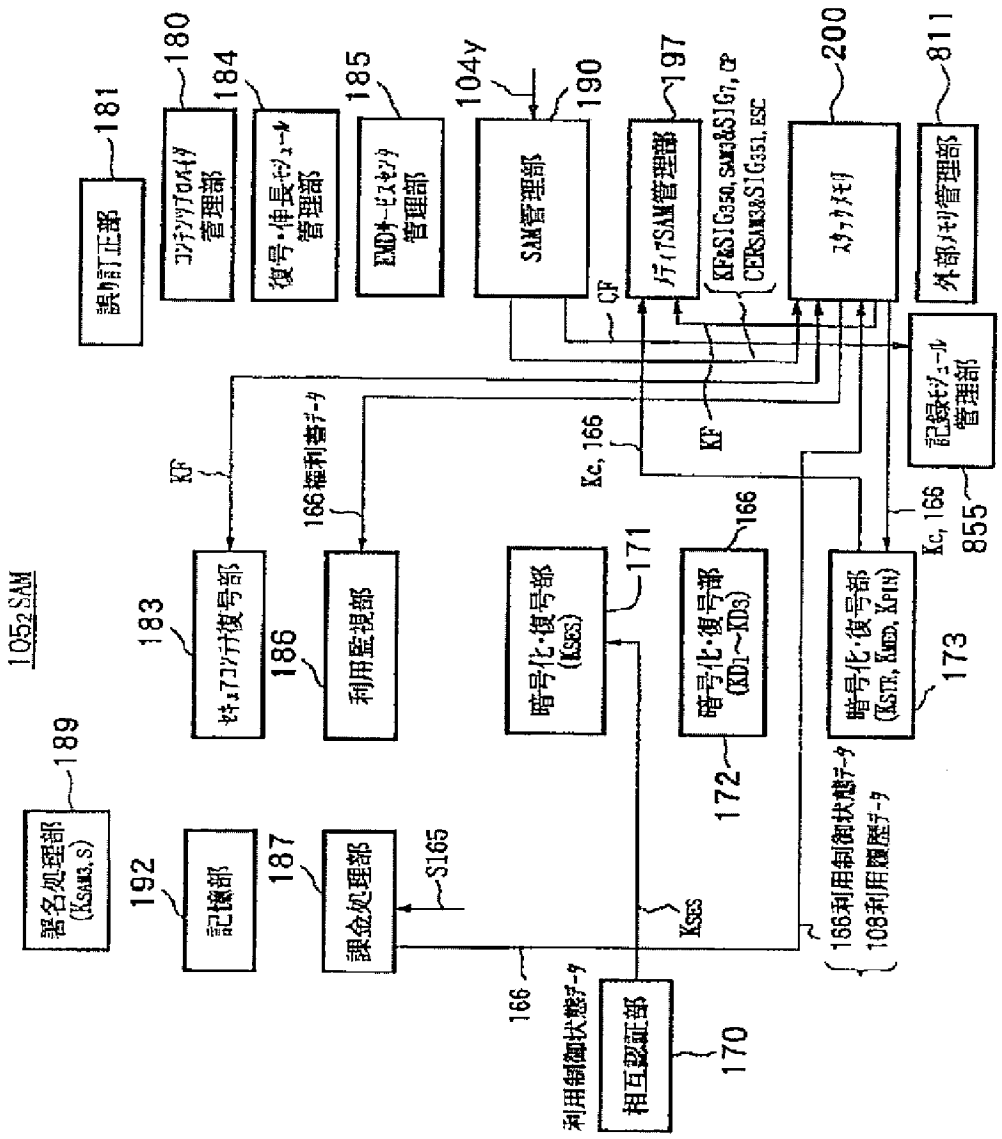
【図３９】


105aSAM
署名処理部
(KSAM3, S)
189
SIGSES, SAM3, SIGSES2, SAM3
192
記憶部
183
セキュアコンテナ復号部
187
課金処理部
186
利用監視部
誤り訂正部
181
コンテンツプロバイダ管理部
180
184
復号・伸長モジュール管理部
185
EMDサービスセンタ管理部
CERSAM3, SIGES1, ESC
171
暗号化・復号部
(KSES)
104v
SAM管理部
190
KF, CF
メディアTSAM管理部
104
197
相互認証部
170
暗号化・復号部
(KD1～KD6)
172
CPASIG6, CP
KFASIG1, CP
CERSCASIG1, ESC
スクラッチメモリ
200
173
暗号化・復号部
(KSTR, KMAC, KPIN)
外部メモリ管理部
811

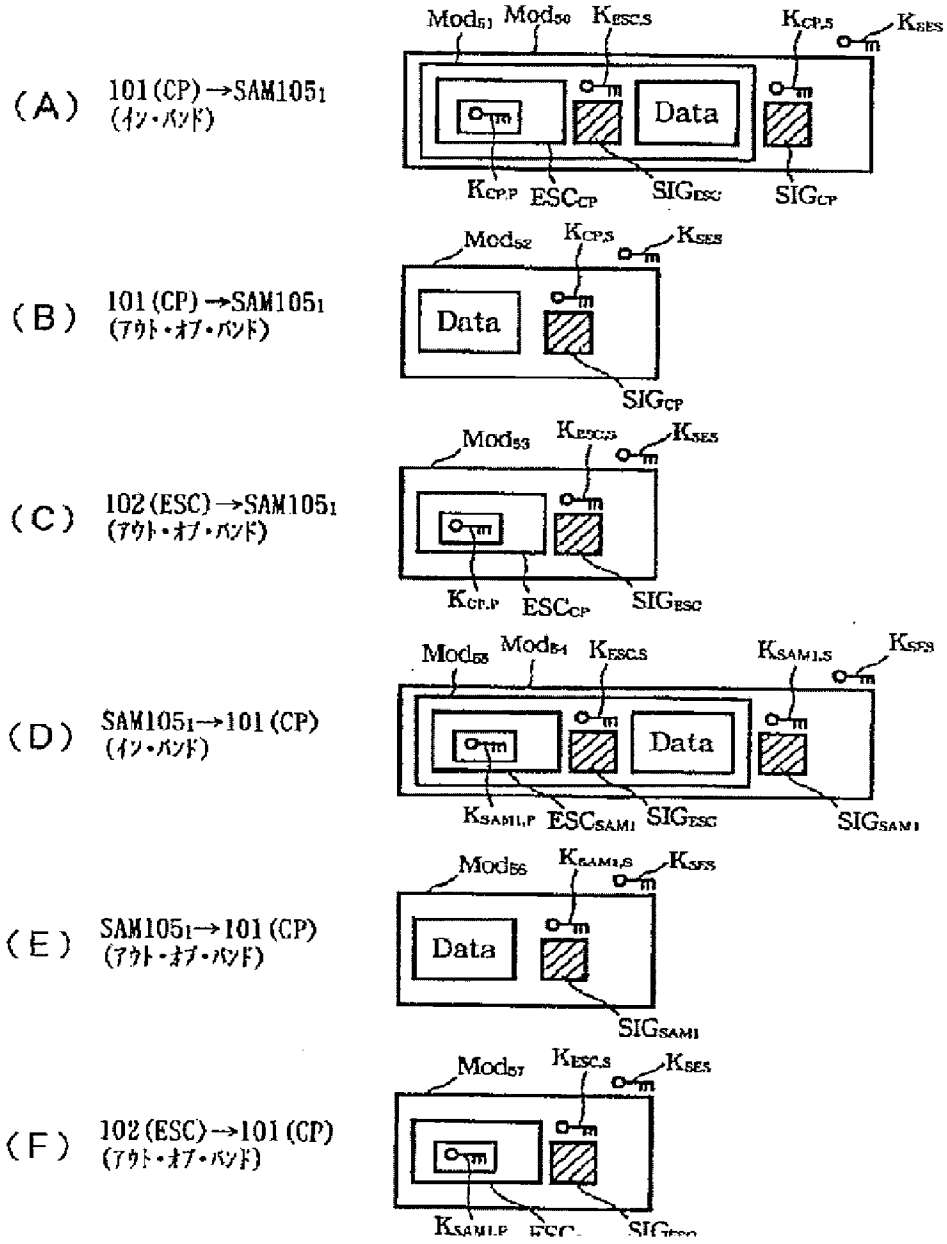
【図４０】


コンテンツファイルACF
105vセキュアコンテナ
コンテンツ鍵データKc
Kc
Kc
Kc
KCP, S
KSAM3, S
(A)
ヘッダ
メタデータ
コンテンツデータ
A/V伸長用ソフトウェア
電子透かし情報モジュール
Meta
C
Soft
WM
SIG6, CP
SIG350, SAM3
配信用鍵データKD1～KD6
キーファイルKF
SDC2
SDC3
KD1～KD6
KESC, S
KCP, S
KSAM3, S
(B)
ヘッダ
UCP
SAMプログラム・ダウンロード・コンテンツ
コンテンツ鍵データKc
IBS利用制御状態データ
SDC1
SIG51, ESC
SIG7, CP
SIG352, SAM3
KESC, S
(C)
公開鍵証明書
SIG351, ESC
KSAM3, S
CERSAM3

【図４１】

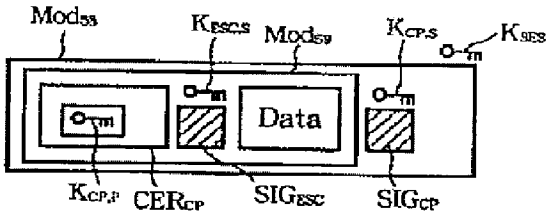

誤訂正部
181
コンテンツDB管理部
180
復号・伸長モジュール管理部
184
EMDサービスセンタ管理部
185
SAM管理部
104y
190
ライブSAM管理部
197
スケジュール
200
外部メモリ管理部
811
記録モジュール管理部
855
CF
KF&SIG350, SAM3&SIG7, CP
CERSAM3&SIG351, ESC
KF
Kc, 166
166権利書データ
KF
Kc, 166
166
171
暗号化・復号部 (KSES)
暗号化・復号部 (KD1～KD3)
172
暗号化・復号部 (KSTR, KMOD, KFIN)
173
166利用制御状態データ
108利用履歴データ
1052 SAM
189
署名処理部 (KSAM3, S)
192
記憶部
187
課金処理部
S165
KSES
166
利用制御状態データ
相互認証部
170
ライブラリ復号部
183
利用監視部
186

【図４２】

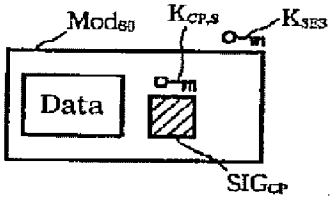

(A) 101(CP)→SAM105₁
(イン・バンド)
Mod₅₁ Mod₅₀ K_ESC,S K_CP,S K_SES
Data
K_CP,P ESC_CP SIG_ESC SIG_CP
(B) 101(CP)→SAM105₁
(アウト・オブ・バンド)
Mod₅₂ K_CP,S K_SES
Data
SIG_CP
(C) 102(ESC)→SAM105₁
(アウト・オブ・バンド)
Mod₅₃ K_ESC,S K_SES
K_CP,P ESC_CP SIG_ESC
(D) SAM105₁→101(CP)
(イン・バンド)
Mod₅₅ Mod₅₄ K_ESC,S K_SAM1,S K_SFS
Data
K_SAM1,P ESC_SAM1 SIG_ESC SIG_SAM1
(E) SAM105₁→101(CP)
(アウト・オブ・バンド)
Mod₅₆ K_SAM1,S K_SFS
Data
SIG_SAM1
(F) 102(ESC)→101(CP)
(アウト・オブ・バンド)
Mod₅₇ K_ESC,S K_SES
K_SAM1,P

【図４３】

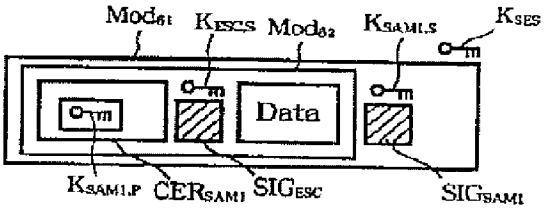
（G）　101(CP)→102(ESC)
(イン・バンド)



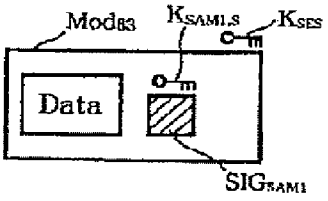
（H）　101(CP)→102(ESC)
(アウト・オブ・バンド)



（I）　SAM105$_1$→102(ESC)
(イン・バンド)

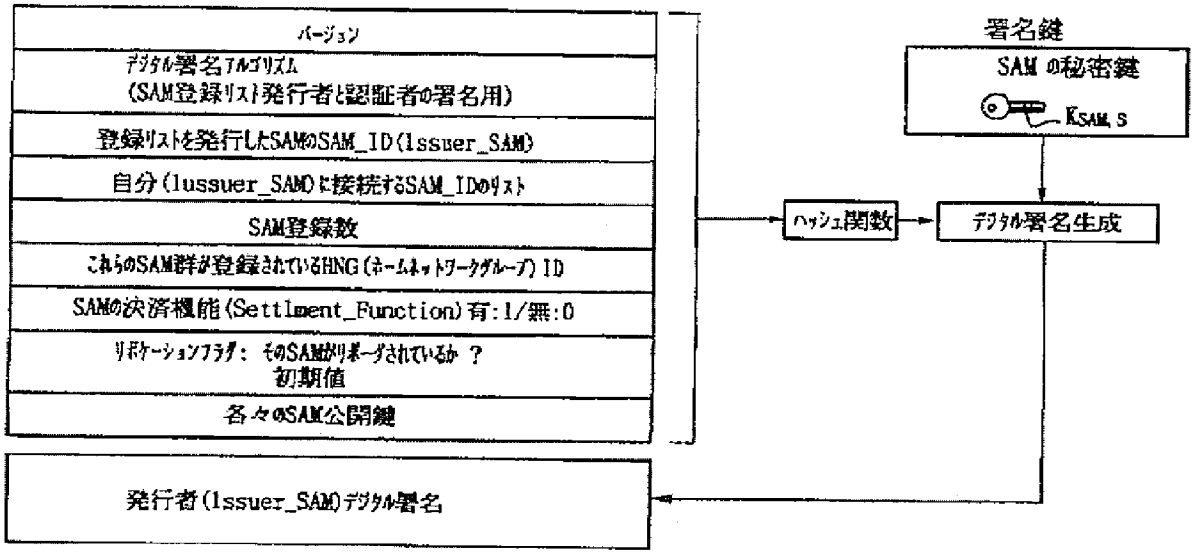


（J）　SAM105$_1$→102(ESC)
(アウト・オブ・バンド)



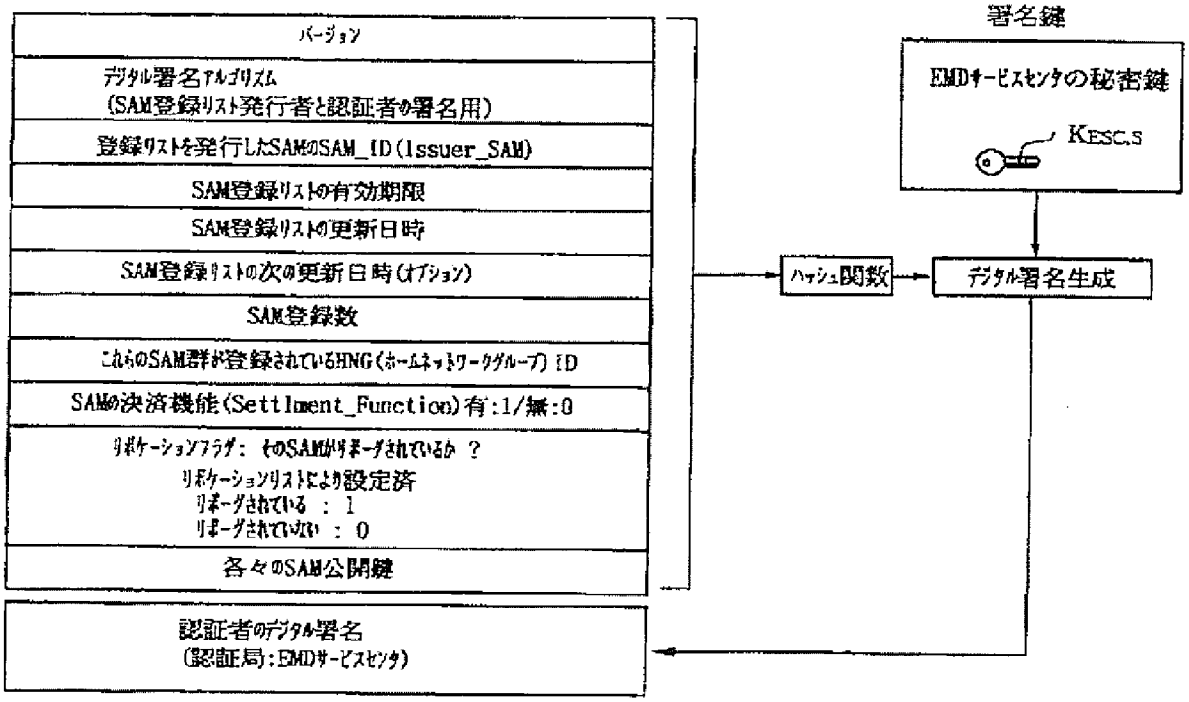
【図４５】

SAM登録リスト(SAM Registration List)(SAM作成)

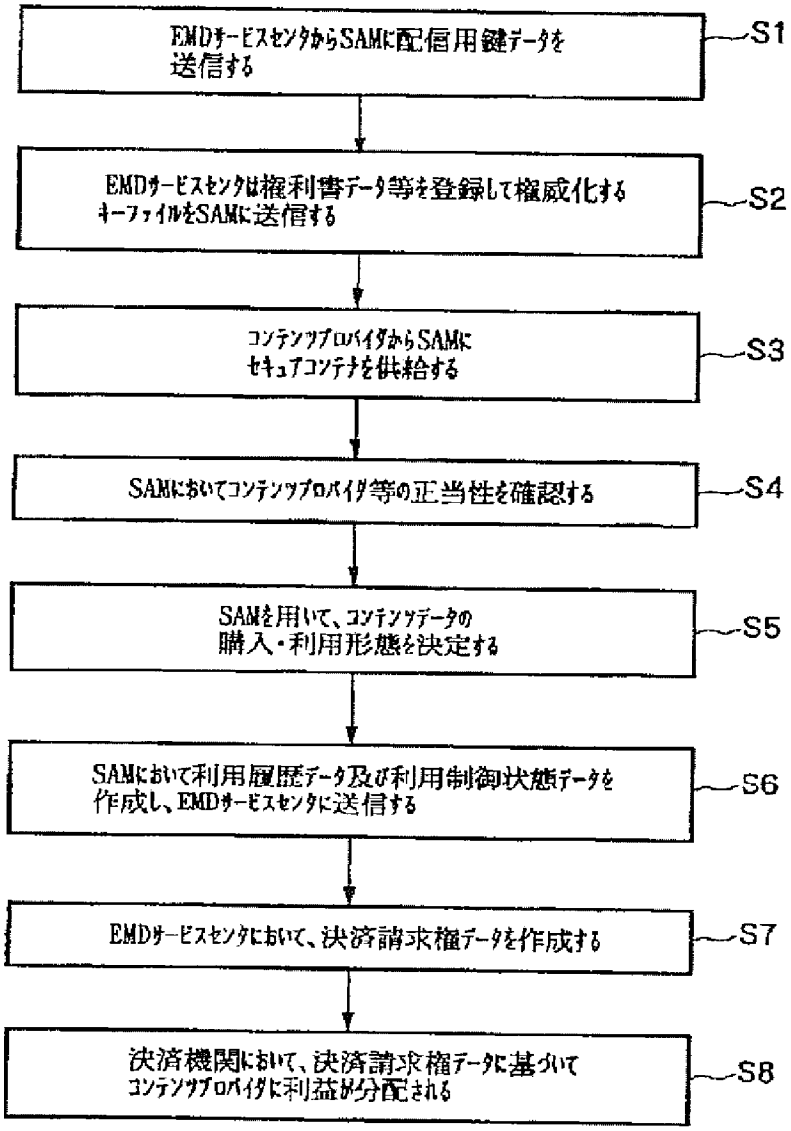


【図４６】

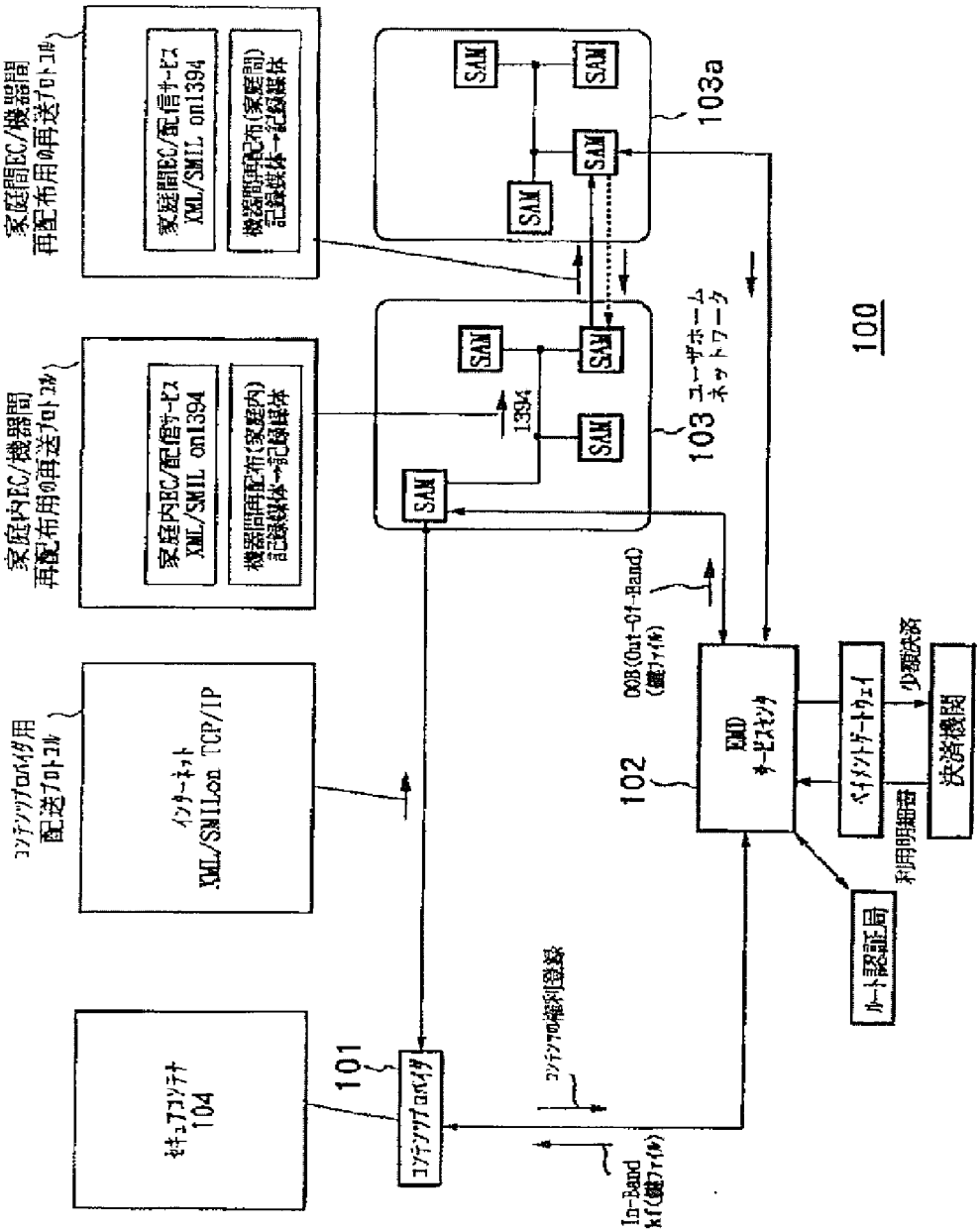
SAM登録リスト(EMDサービスセンタが作成)



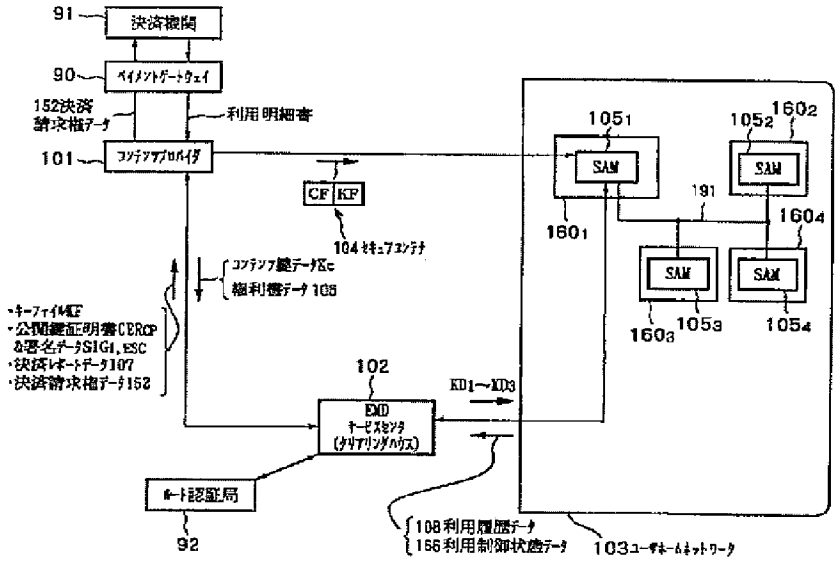
【図４７】


EMDサービスセンタからSAMに配信用鍵データを送信する
S1
EMDサービスセンタは権利書データ等を登録して権威化するキーファイルをSAMに送信する
S2
コンテンツプロバイダからSAMにセキュアコンテナを供給する
S3
SAMにおいてコンテンツプロバイダ等の正当性を確認する
S4
SAMを用いて、コンテンツデータの購入・利用形態を決定する
S5
SAMにおいて利用履歴データ及び利用制御状態データを作成し、EMDサービスセンタに送信する
S6
EMDサービスセンタにおいて、決済請求権データを作成する
S7
決済機関において、決済請求権データに基づいてコンテンツプロバイダに利益が分配される
S8

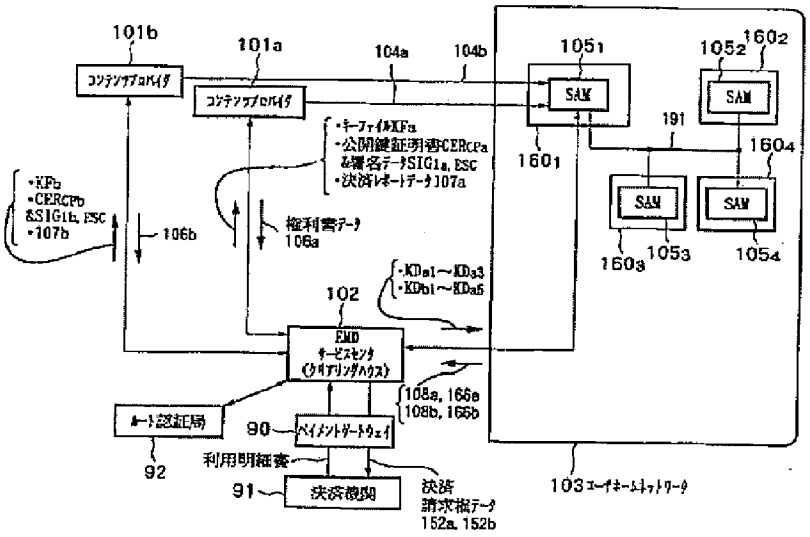
【図４８】


家庭間EC/機器間
再配布用の再送プロトコル
家庭間EC/配信サービス
XML/SMIL on1394
機器間再配布(家庭間)
記録媒体→記録媒体
家庭内EC/機器間
再配布用の再送プロトコル
家庭内EC/配信サービス
XML/SMIL on1394
機器間再配布(家庭内)
記録媒体→記録媒体
コンテンツプロバイダ用
配送プロトコル
インターネット
XML/SMILon TCP/IP
セキュアコンテナ
104
101
コンテンツプロバイダ
コンテンツの権利登録
In-Band
Key(鍵ファイル)
SAM
1394
103a
103
ユーザホーム
ネットワーク
100
OOB(Out-Of-Band)
(鍵ファイル)
102
RMD
サービスセンタ
ペイメントゲートウェイ
少額決済
利用明細書
決済機関
ルート認証局

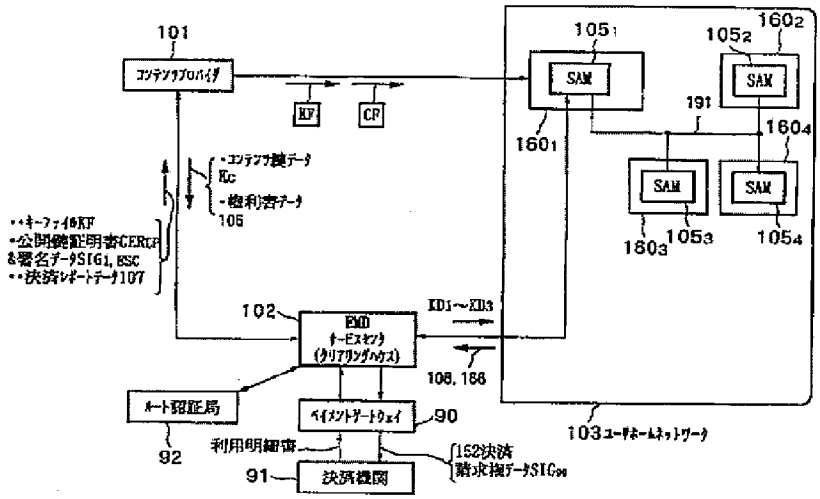
【図４９】


91
決済機関
90
ペイメントゲートウェイ
152決済
請求権データ
利用明細書
101
コンテンツプロバイダ
CF
KF
104 セキュアコンテナ
コンテンツ鍵データKc
権利書データ 106
・キーファイルKF
・公開鍵証明書CERCP
&署名データSIG1, ESC
・決済レポートデータ107
・決済請求権データ152
102
EMD
サービスセンタ
(クリアリングハウス)
KD1～KD3
ルート認証局
92
108利用履歴データ
156利用制御状態データ
103ユーザホームネットワーク
SAM
1051
1052
1602
1601
191
1604
1603
1053
1054

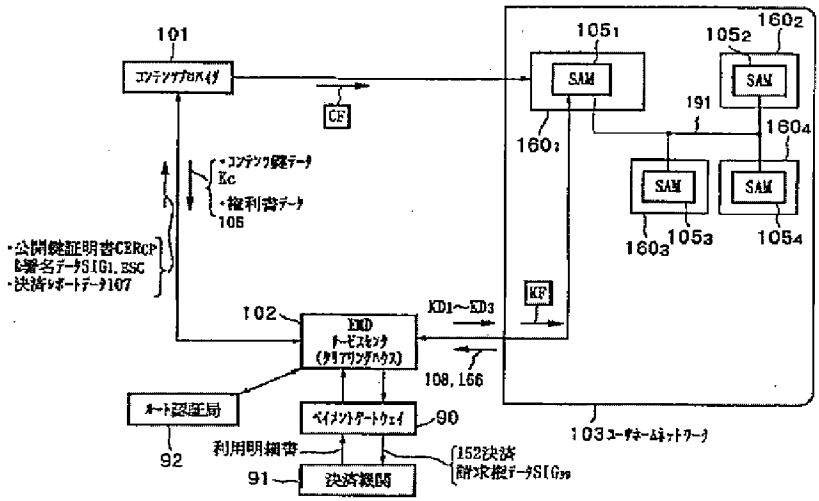
【図５０】


101b
101a
104a
104b
コンテンツプロバイダ
コンテンツプロバイダ
・キーファイルKFa
・公開鍵証明書CERCPa
&署名データSIG1a, ESC
・決済レポートデータ107a
・KPb
・CERCPb
&SIG1b, ESC
・107b
106b
権利書データ
106a
・KDa1～KDa3
・KDb1～KDa5
102
EMD
サービスセンタ
(クリアリングハウス)
108a, 166a
108b, 166b
ルート認証局
90
ペイメントゲートウェイ
92
利用明細書
91
決済機関
決済
請求権データ
152a, 152b
103ユーザホームネットワーク
SAM
1051
1052
1602
1601
191
1604
1603
1053
1054

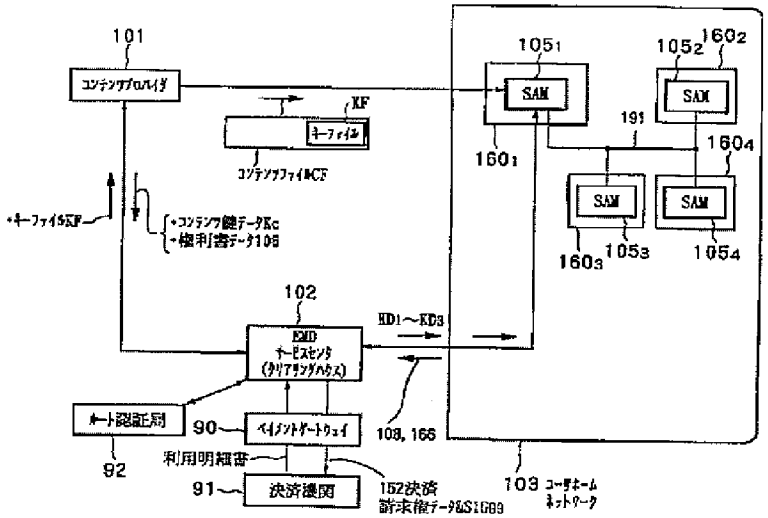
【図５１】


101
コンテンツプロバイダ
KF
CF
・コンテンツ鍵データ
Kc
・権利書データ
105
・・キーファイルKF
・公開鍵証明書CERCP
&署名データSIG1, ESC
・・決済レポートデータ107
102
EMD
サービスセンタ
(クリアリングハウス)
KD1～KD3
108, 166
オート認証局
92
ペイメントゲートウェイ
90
利用明細書
152決済
要求書データSIG99
91
決済機関
1051
1052
1602
SAM
191
1601
1604
1603
1053
1054
103ユーザホームネットワーク

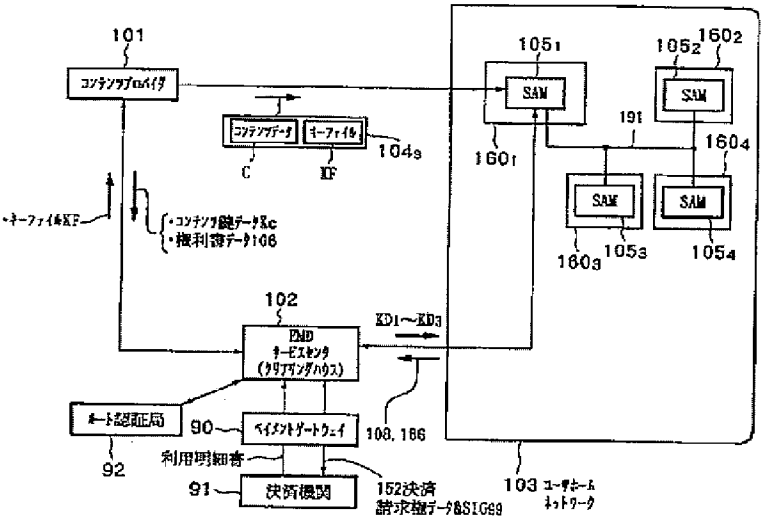
【図５２】


101
コンテンツプロバイダ
CF
・コンテンツ鍵データ
Kc
・権利書データ
105
・公開鍵証明書CERCP
&署名データSIG1, ESC
・決済レポートデータ107
102
EMD
サービスセンタ
(クリアリングハウス)
KD1～KD3
KF
108, 166
オート認証局
92
ペイメントゲートウェイ
90
利用明細書
152決済
要求書データSIG99
91
決済機関
1051
1052
1602
SAM
191
1601
1604
1603
1053
1054
103ユーザホームネットワーク

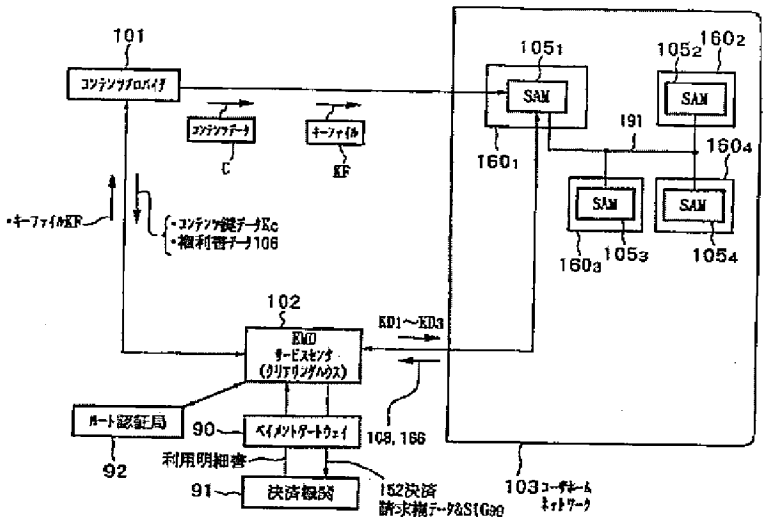
【図５３】


101
コンテンツプロバイダ
KF
キーファイル
コンテンツファイルCF
キーファイルKF
・コンテンツ鍵データKc
・権利書データ106
102
EMD
サービスセンタ
(クリアリングハウス)
ネット認証局
90
ペイメントゲートウェイ
92
利用明細書
91
決済機関
HD1～KD3
108, 166
152決済
請求権データ&SIG99
103 ユーザホーム
ネットワーク
105₁
SAM
160₁
105₂
160₂
191
160₄
160₃
105₃
105₄

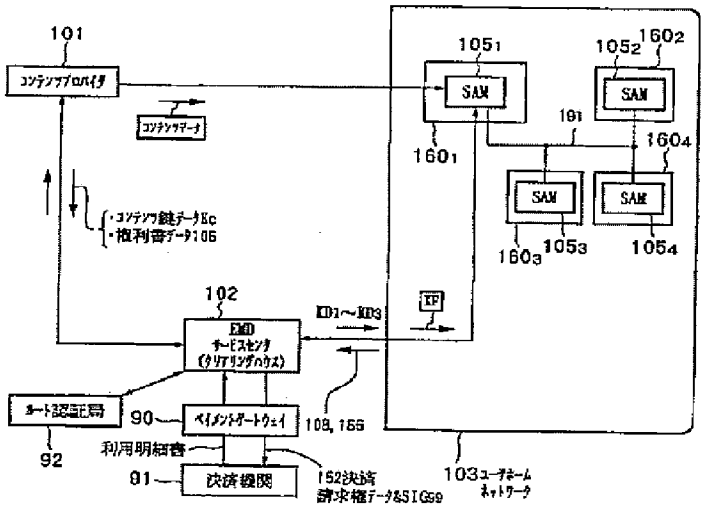
【図５４】


101
コンテンツプロバイダ
コンテンツデータ
キーファイル
104₉
C
KF
キーファイルKF
・コンテンツ鍵データKc
・権利書データ106
102
EMD
サービスセンタ
(クリアリングハウス)
ネット認証局
90
ペイメントゲートウェイ
92
利用明細書
91
決済機関
KD1～KD3
108, 166
152決済
請求権データ&SIG99
103 ユーザホーム
ネットワーク
105₁
SAM
160₁
105₂
160₂
191
160₄
160₃
105₃
105₄

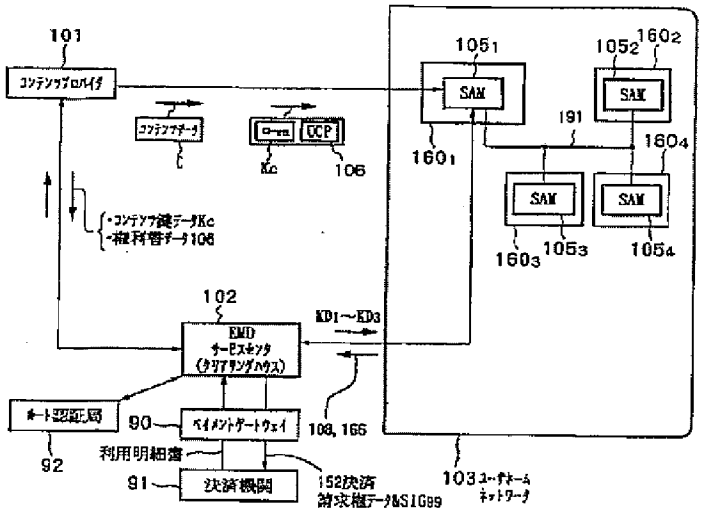
【図５５】


101
コンテンツプロバイダ
コンテンツデータ
C
キーファイル
KF
・キーファイルKF
・コンテンツ鍵データKc
・複利書データ106
1051
SAM
1601
1052
1602
SAM
191
1604
SAM
SAM
1603
1053
1054
102
EMD
サービスセンタ
(クリアリングハウス)
KD1～KD3
ポート認証局
92
90
ペイメントゲートウェイ
108, 166
利用明細書
91
決済機関
152決済
請求権データ&SIG99
103ユーザホーム
ネットワーク

【図５６】


101
コンテンツプロバイダ
コンテンツデータ
・コンテンツ鍵データKc
・複利書データ106
1051
SAM
1601
1052
1602
SAM
191
1604
SAM
SAM
1603
1053
1054
102
KD1～KD3
KF
EMD
サービスセンタ
(クリアリングハウス)
ポート認証局
92
90
ペイメントゲートウェイ
108, 166
利用明細書
91
決済機関
152決済
請求権データ&SIG99
103ユーザホーム
ネットワーク

【図５７】

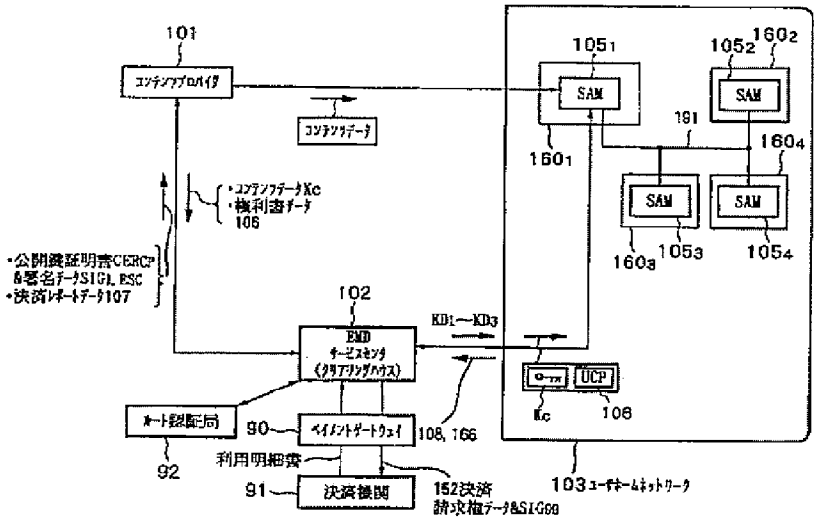


【図７７】

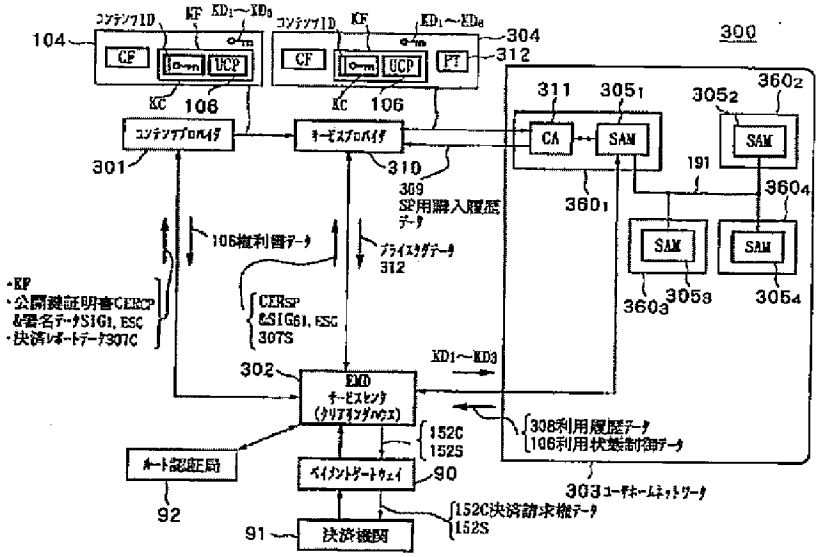
スタックメモリ200の記憶データ

コンテンツ鍵データKc
権利書データ(UCP)106
不揮発性メモリ201のロック鍵データK_{LOC}
コンテンツプロバイダ301の公開鍵証明書データCER_{CP}
サービスプロバイダ301の公開鍵証明書データCER_{SP}
利用制御情状態データ(UCS)166
SAMプログラム・ダウンロード・コンテナSD_1～SDC_3
プライスタグデータ312

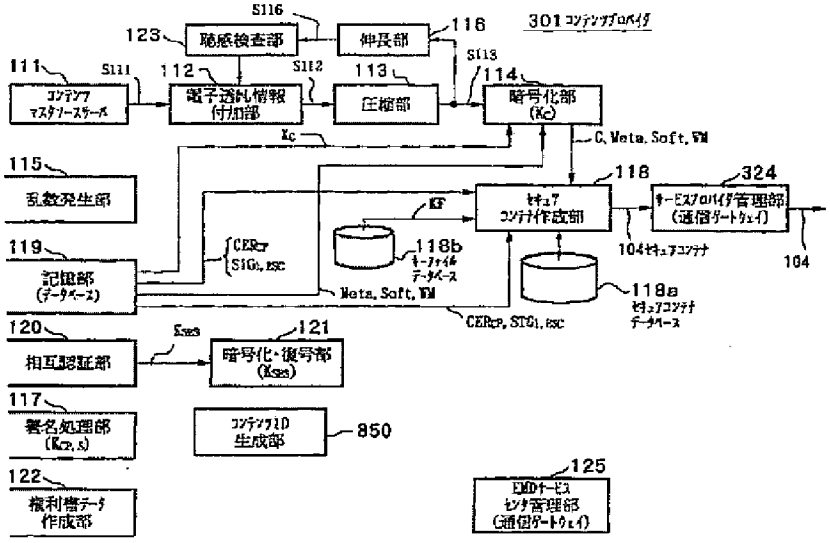
【図５８】



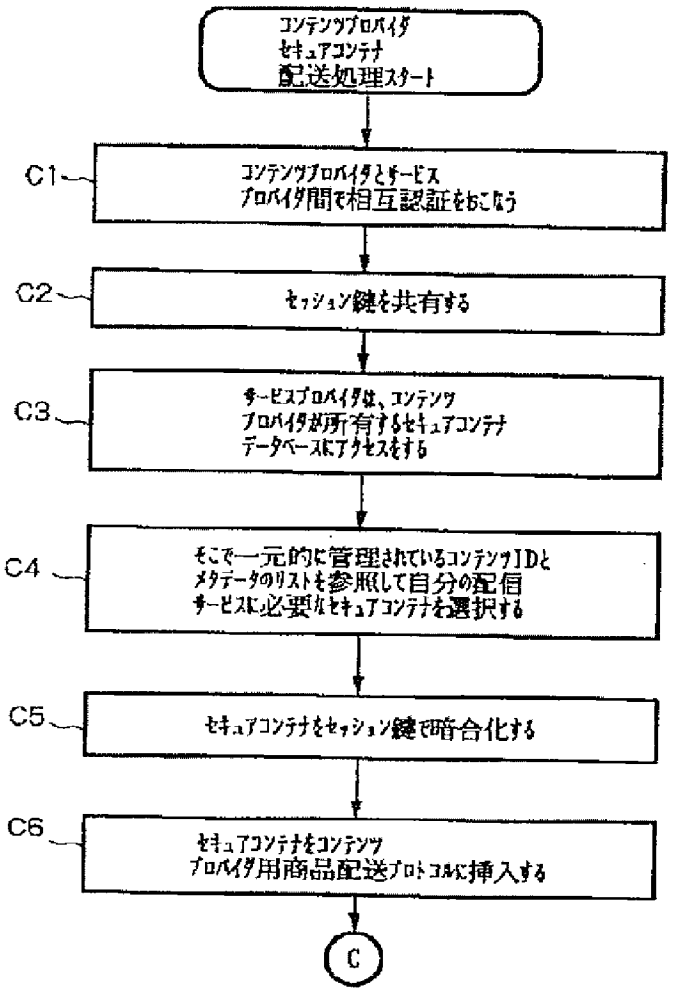
【図５９】


104
CF
UCP
KC
106
KF
KD1～KD3
304
312
PT
300
311
305₁
305₂
360₂
CA
SAM
301
310
309
191
360₄
360₁
360₃
305₃
305₄
106権利書データ
プライスタグデータ
312
KF
・公開鍵証明書CERCP
&署名データSIG1, ESC
・決済レポートデータ307C
CERSP
&SIG61, ESC
307S
302
KD1～KD3
EMD
サービスセンタ
(クリアリングハウス)
308利用履歴データ
106利用状態制御データ
303ユーザホームネットワーク
ポート認証局
92
152C
152S
ペイメントゲートウェイ
90
152C決済請求権データ
152S
91
決済機関

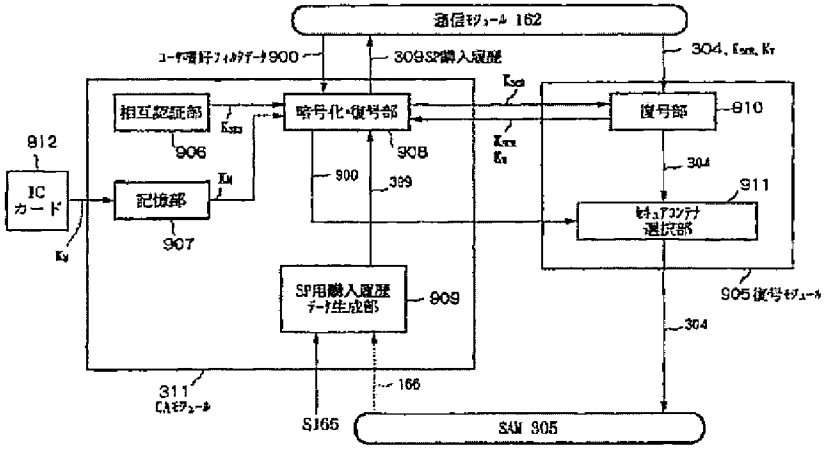
【図６０】


S116
123
聴感検査部
伸長部
116
301コンテンツプロバイダ
111
S111
112
S112
113
S113
114
コンテンツ
マスターデータベース
電子透かし情報
付加部
圧縮部
暗号化部
(Kc)
Kc
C, Meta, Soft, WM
115
乱数発生部
KF
118
セキュア
コンテナ作成部
324
サービスプロバイダ管理部
(通信ゲートウェイ)
119
CERCP
SIG1, ESC
118b
キーファイル
データベース
104セキュアコンテナ
104
記憶部
(データベース)
Meta, Soft, WM
CERCP, SIG1, ESC
118a
セキュアコンテナ
データベース
120
Kses
121
相互認証部
暗号化・復号部
(Kses)
117
署名処理部
(Kcp, s)
コンテンツID
生成部
850
125
EMDサービス
センタ管理部
(通信ゲートウェイ)
122
権利書データ
作成部

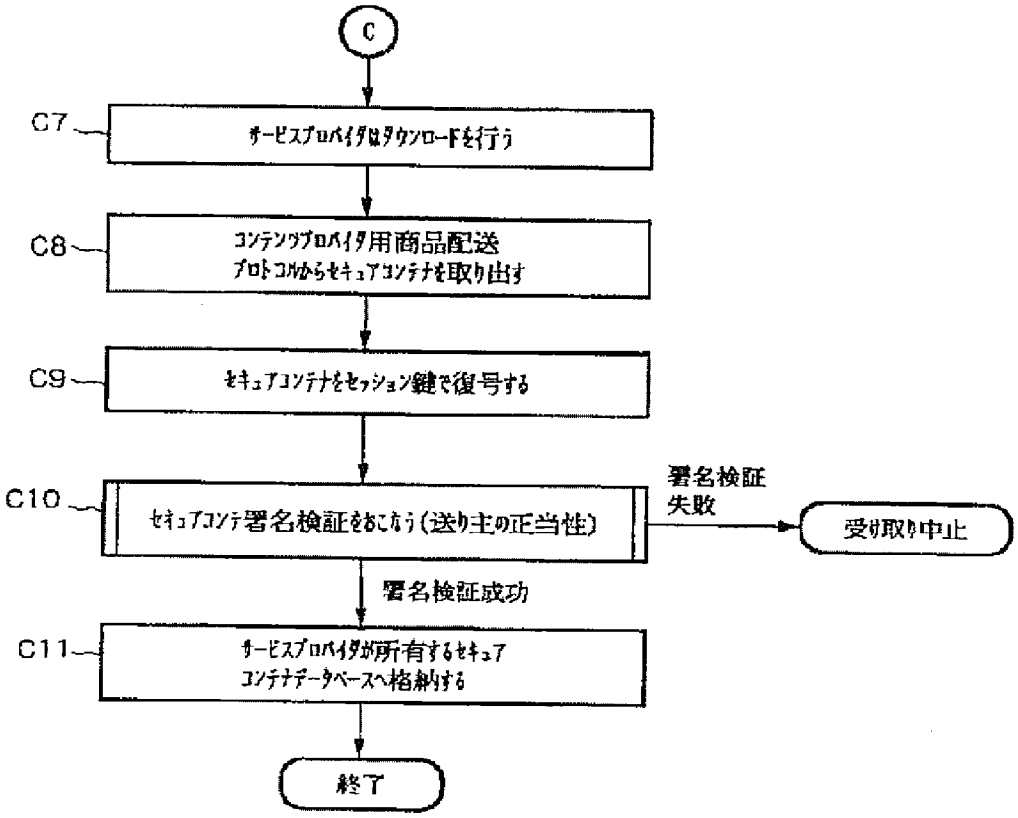
【図６１】


コンテンツプロバイダ
セキュアコンテナ
配送処理スタート
C1
コンテンツプロバイダとサービス
プロバイダ間で相互認証をおこなう
C2
セッション鍵を共有する
C3
サービスプロバイダは、コンテンツ
プロバイダが所有するセキュアコンテナ
データベースにアクセスをする
C4
そこで一元的に管理されているコンテンツIDと
メタデータのリストを参照して自分の配信
サービスに必要なセキュアコンテナを選択する
C5
セキュアコンテナをセッション鍵で暗合化する
C6
セキュアコンテナをコンテンツ
プロバイダ用商品配送プロトコルに挿入する
C

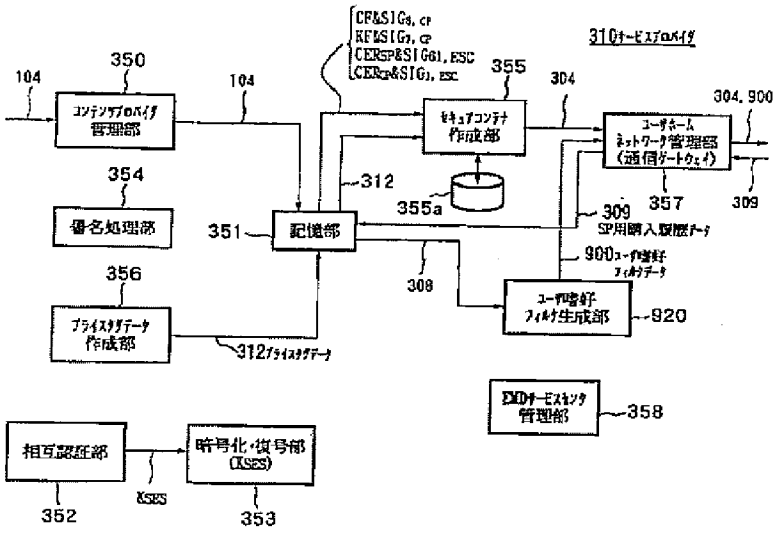
【図７５】


通信モジュール 162
ユーザ嗜好フィルタデータ900
309SP購入履歴
304、Kmn、Kr
相互認証部
906
暗号化・復号部
908
復号部
910
912
ICカード
記憶部
907
900
309
911
セキュアコンテナ選択部
304
SP用購入履歴データ生成部
909
905復号モジュール
304
311
CAモジュール
S165
166
SAM 305

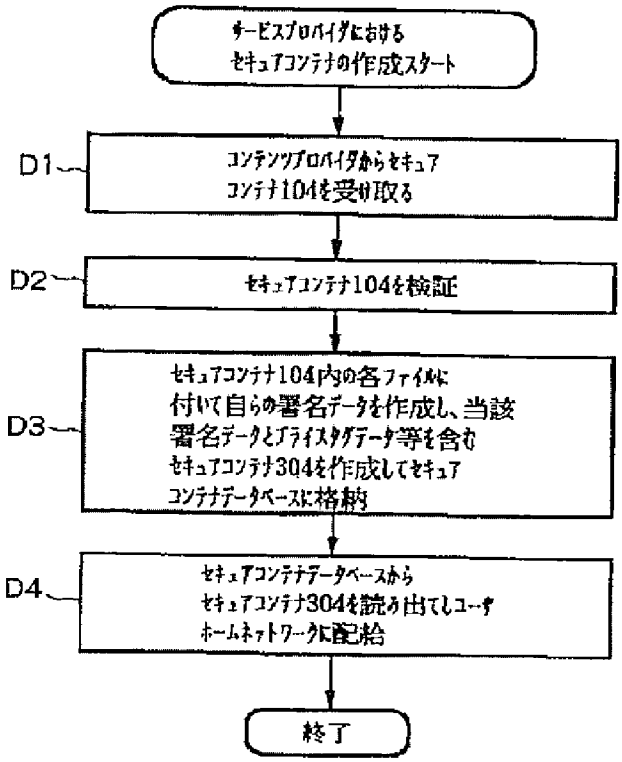
【図６２】


C
C7
サービスプロバイダはダウンロードを行う
C8
コンテンツプロバイダ用商品配送
プロトコルからセキュアコンテナを取り出す
C9
セキュアコンテナをセッション鍵で復号する
C10
セキュアコンテナ署名検証をおこなう(送り主の正当性)
署名検証
失敗
受け取り中止
署名検証成功
C11
サービスプロバイダが所有するセキュア
コンテナデータベースへ格納する
終了

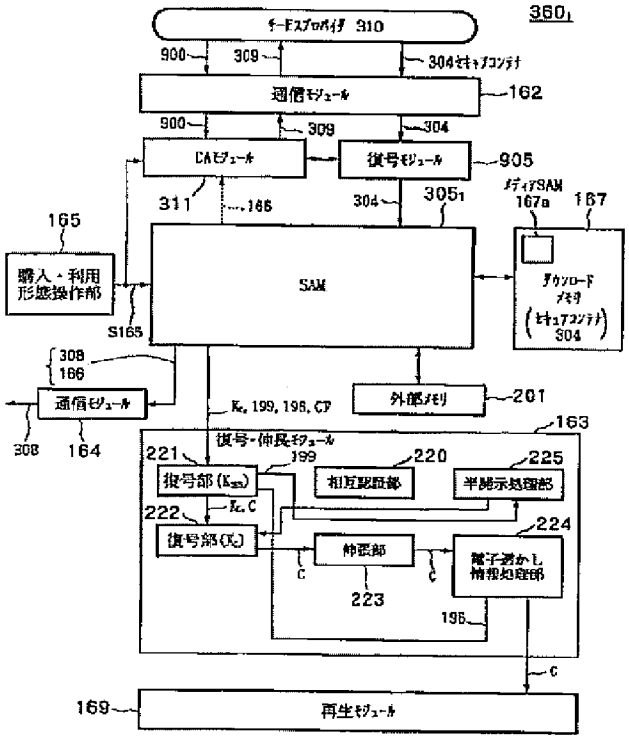
【図６３】


CF&SIG3, CP
RF&SIG2, CP
CERSP&SIG61, ESC
CERCP&SIG1, ESC
310サービスプロバイダ
350
104
104
355
304
304, 900
354
312
355a
309
357
309
351
記憶部
309
SP用購入履歴データ
900
308
356
312プライスタグデータ
920
358
352
XSES
353

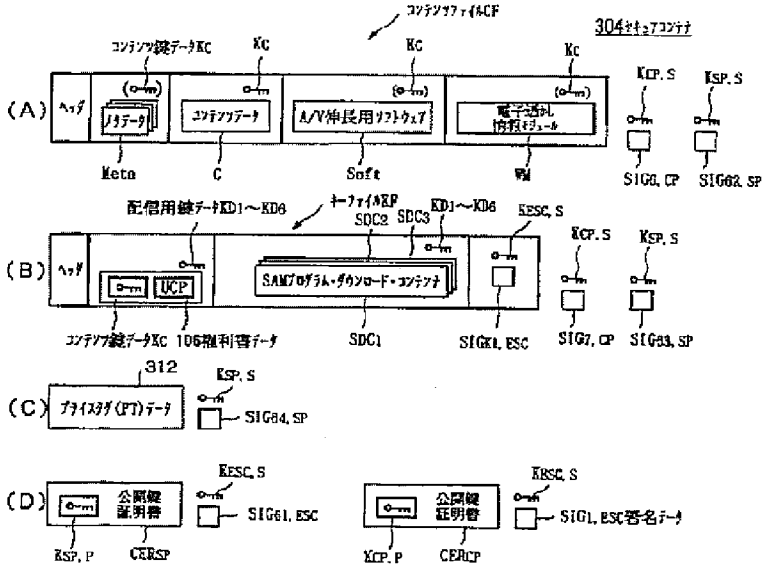
【図６４】


サービスプロバイダにおける
セキュアコンテナの作成スタート
D1
コンテンツプロバイダからセキュア
コンテナ104を受け取る
D2
セキュアコンテナ104を検証
D3
セキュアコンテナ104内の各ファイルに
付いて自らの署名データを作成し、当該
署名データとプライスタグデータ等を含む
セキュアコンテナ304を作成してセキュア
コンテナデータベースに格納
D4
セキュアコンテナデータベースから
セキュアコンテナ304を読み出してユーザ
ホームネットワークに配給
終了

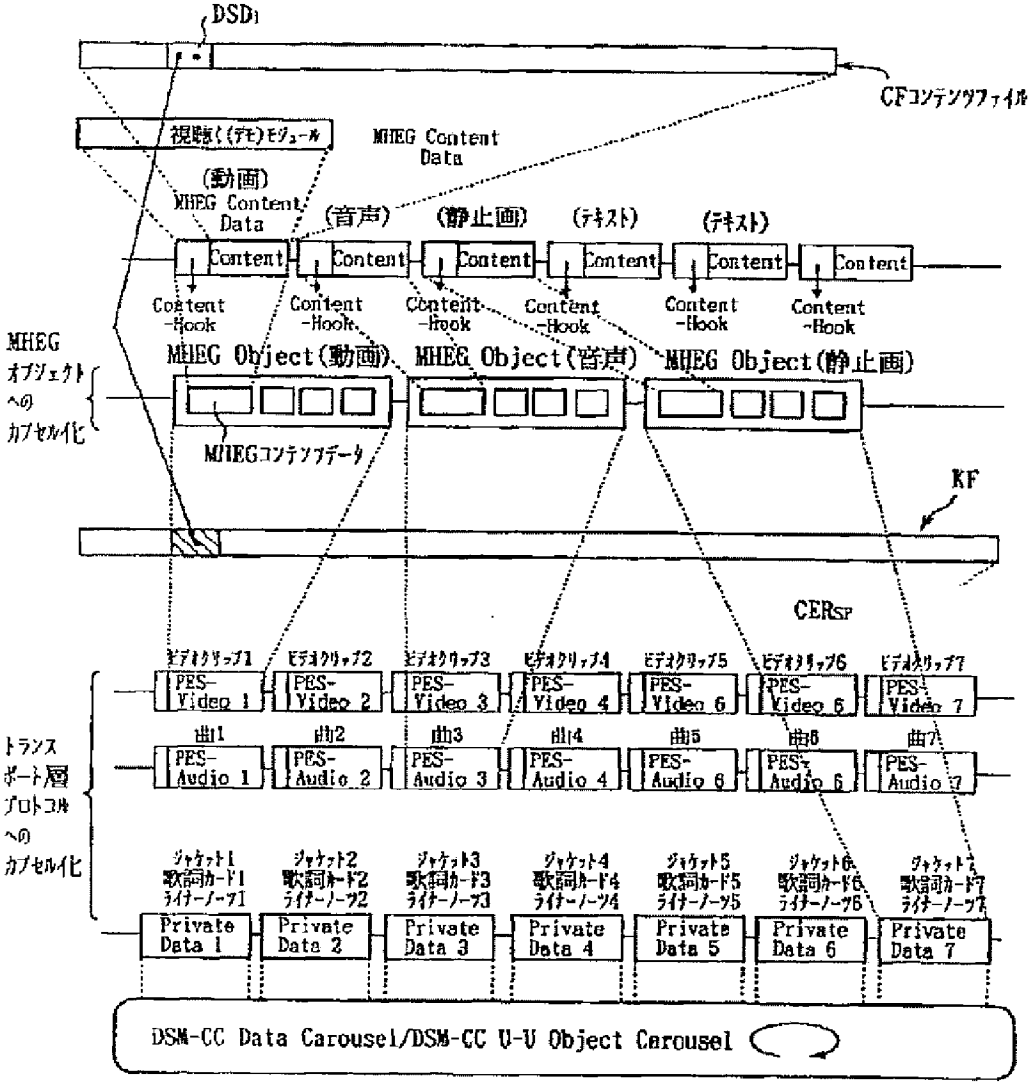
【図７４】


360₁
サービスプロバイダ 310
900
309
304セキュアコンテナ
通信モジュール
162
CAモジュール
復号モジュール
905
311
166
304
305₁
メディアSAM
167a
167
165
購入・利用
形態操作部
SAM
ダウンロード
メモリ
(セキュアコンテナ
304)
S165
308
166
通信モジュール
308
164
K, 199, 195, CP
外部メモリ
201
163
復号・伸長モジュール
221
199
220
225
復号部 (K_enc)
相互認証部
半導体処理部
222
K, C
復号部 (K_dec)
224
伸張部
電子署かし
情報処理部
C
223
195
C
169
再生モジュール

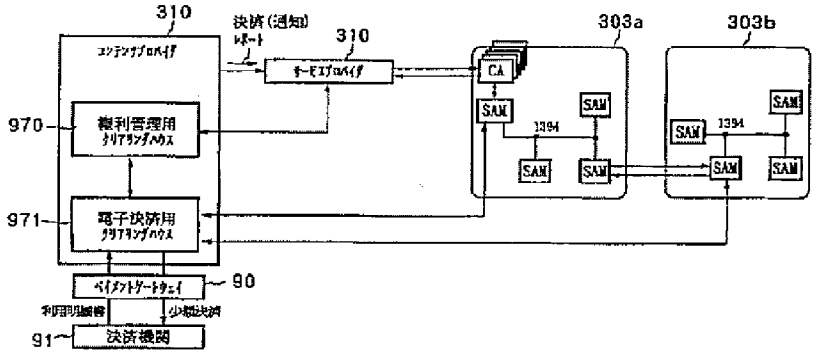
【図６５】


コンテンツファイルCF
304セキュアコンテナ
コンテンツ鍵データKC
Kc
Kc
Kc
KCP, S
KSP, S
(A)
ヘッダ
メタデータ
コンテンツデータ
A/V伸長用ソフトウェア
電子透かし
情報モジュール
Meta
C
Soft
Wd
SIG0, CP
SIG02, SP
配信用鍵データKD1～KD6
キーファイルKF
SDC2
SDC3
KD1～KD6
KESC, S
KCP, S
KSP, S
(B)
ヘッダ
UCP
SAMプログラム・ダウンロード・コンテンツ
コンテンツ鍵データKC
106種利害データ
SDC1
SIG61, ESC
SIG7, CP
SIG63, SP
312
KSP, S
(C)
プライスタグ(PT)データ
SIG64, SP
KESC, S
(D)
公開鍵
証明書
SIG61, ESC
RSP, P
CERSP
KESC, S
公開鍵
証明書
SIG1, ESC署名データ
KCP, P
CERCP

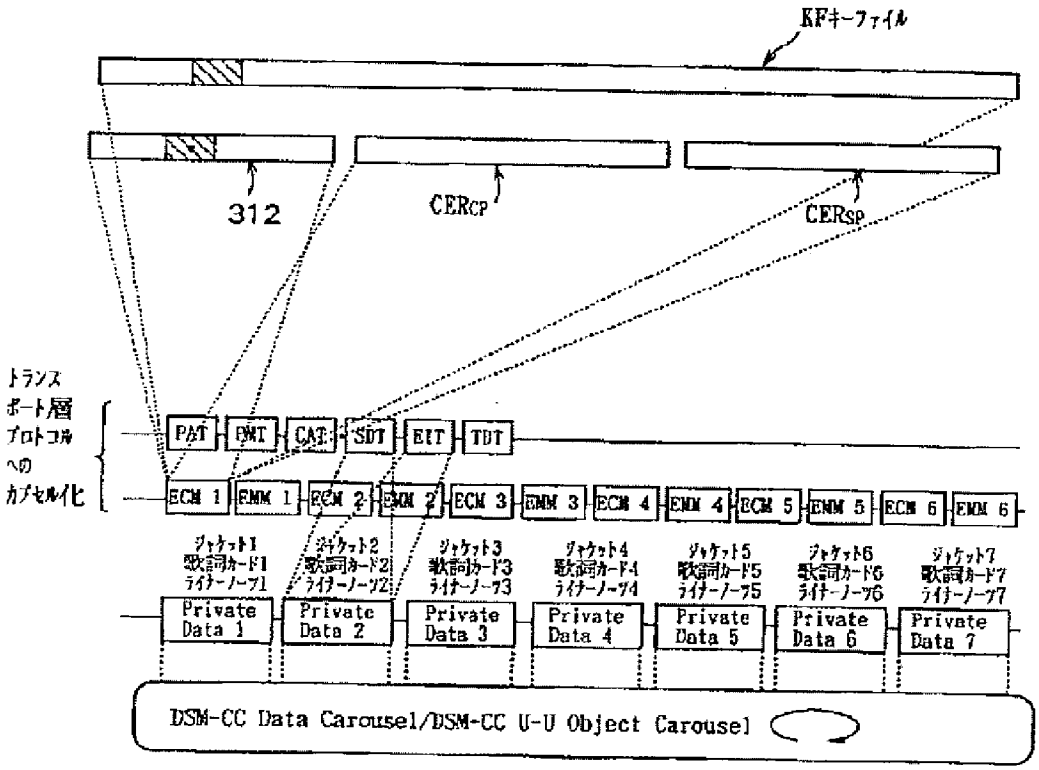
【図６６】


DSD1
CFコンテンツファイル
視聴(デモ)モジュール
MHEG Content Data
(動画)
MHEG Content Data
(音声)
(静止画)
(テキスト)
(テキスト)
Content
Content Hook
MHEG オブジェクトへのカプセル化
MHEG Object(動画)
MHEG Object(音声)
MHEG Object(静止画)
MHEGコンテンツデータ
KF
CERSP
トランスポート層プロトコルへのカプセル化
PES-Video 1
PES-Video 2
PES-Video 3
PES-Video 4
PES-Video 5
PES-Video 6
PES-Video 7
曲1
曲2
曲3
曲4
曲5
曲6
曲7
PES-Audio 1
PES-Audio 2
PES-Audio 3
PES-Audio 4
PES-Audio 5
PES-Audio 6
PES-Audio 7
Private Data 1
Private Data 2
Private Data 3
Private Data 4
Private Data 5
Private Data 6
Private Data 7
DSM-CC Data Carousel/DSM-CC U-U Object Carousel

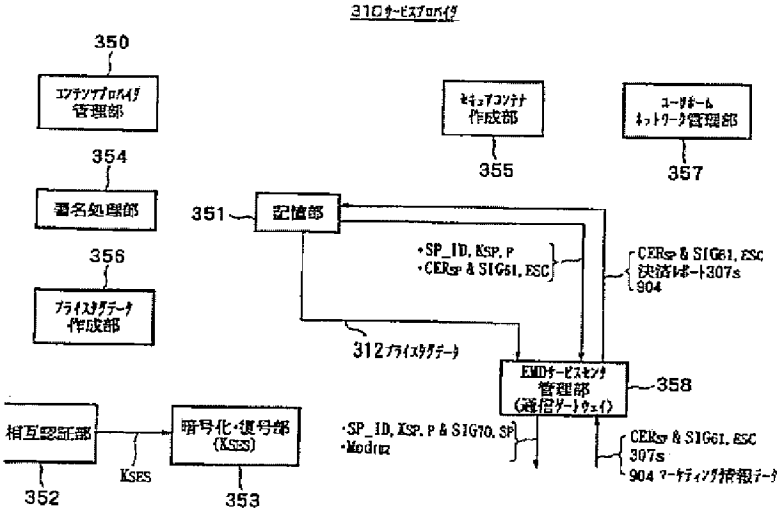
【図１１０】


310
310
303a
303b
970
971
90
91
CA
SAM
1394
決済機関

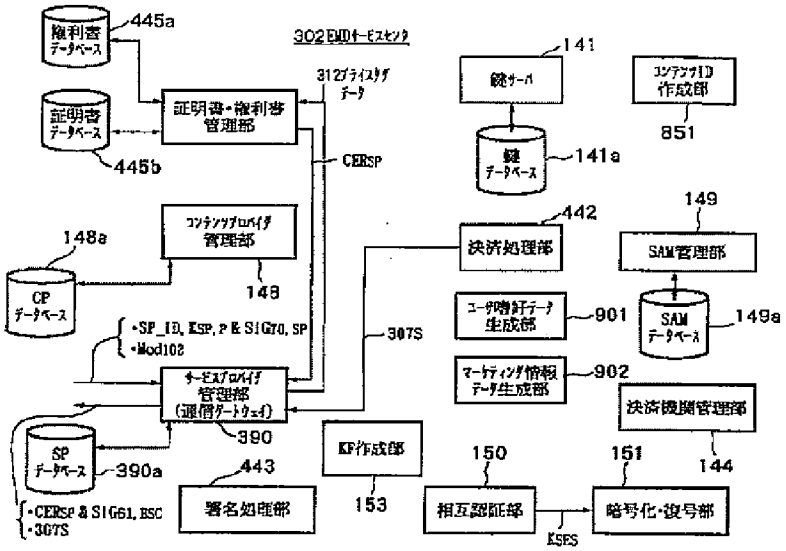
【図６７】


KFキーファイル
312
CERCP
CERSP
トランスポート層プロトコルへのカプセル化
PAT
PMT
CAT
SDT
EIT
TDT
ECM 1
EMM 1
ECM 2
EMM 2
ECM 3
EMM 3
ECM 4
EMM 4
ECM 5
EMM 5
ECM 6
EMM 6
Private Data 1
Private Data 2
Private Data 3
Private Data 4
Private Data 5
Private Data 6
Private Data 7
DSM-CC Data Carousel/DSM-CC U-U Object Carousel

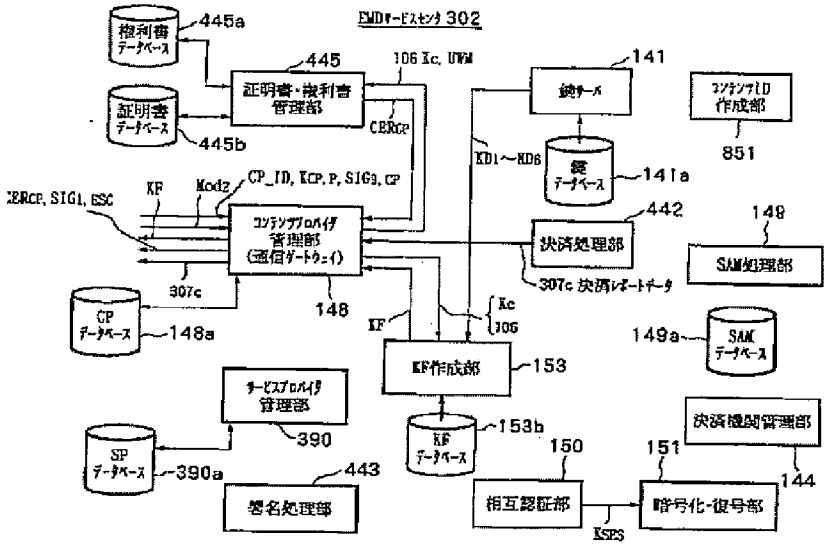
【図６８】


350
355
357
354
351
記憶部
356
SP_ID, KSP, P
CERSP & SIG61, ESC
312
358
352
KSES
353
CERSP & SIG61, ESC
307s
904

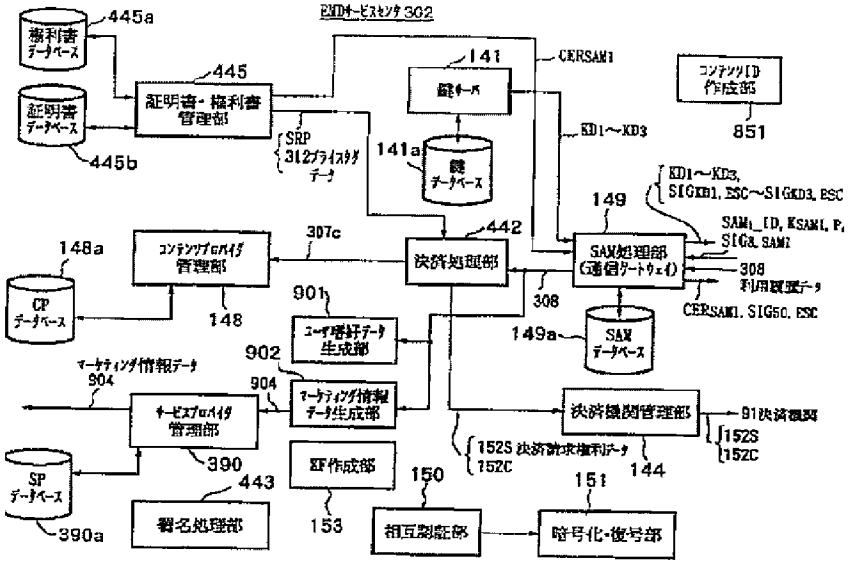
【図７０】


権利書データベース
445a
証明書データベース
445b
証明書・権利書管理部
312プライスタグデータ
CERSP
302 EMDサービスセンタ
鍵サーバ
141
鍵データベース
141a
コンテンツID作成部
851
コンテンツプロバイダ管理部
148
148a
CPデータベース
決済処理部
442
149
SAM管理部
SAMデータベース
149a
ユーザ嗜好データ生成部
901
マーケティング情報データ生成部
902
決済機関管理部
144
307S
サービスプロバイダ管理部（通信ゲートウェイ）
390
SPデータベース
390a
KF作成部
153
150
151
相互認証部
暗号化・復号部
KSES
443
署名処理部
•SP_ID, KSP, P & SIG70, SP
•Mod102
•CERSP & SIG61, BSC
•307S

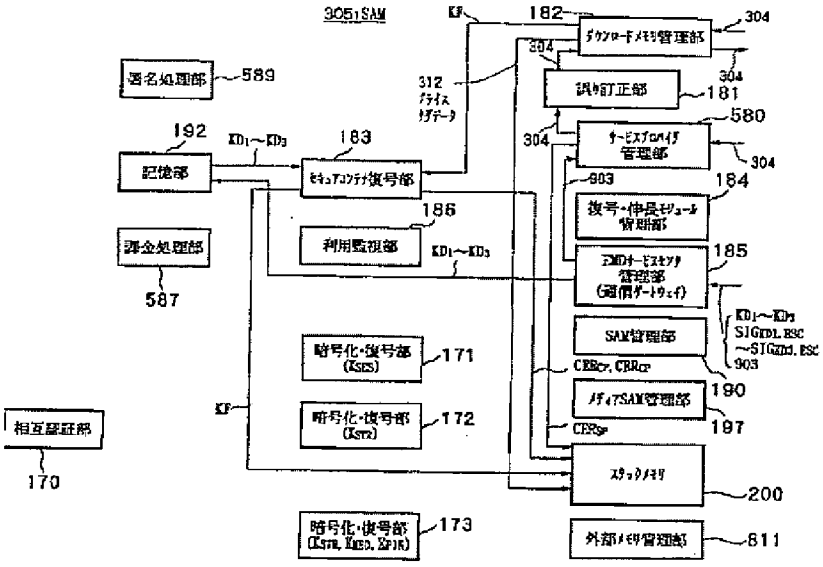
【図７１】


権利書データベース
445a
証明書データベース
445b
EMDサービスセンタ 302
証明書・権利書管理部
445
106 Kc, UWM
CERCP
鍵サーバ
141
鍵データベース
141a
KD1～KD6
コンテンツID作成部
851
CERCP, SIG1, BSC
KF
Mod2
CP_ID, KCP, P, SIG3, CP
コンテンツプロバイダ管理部（通信ゲートウェイ）
307c
148
CPデータベース
148a
決済処理部
442
307c 決済レポートデータ
SAM処理部
148
149a
SAMデータベース
Kc
306
KF作成部
153
サービスプロバイダ管理部
390
KFデータベース
153b
SPデータベース
390a
署名処理部
443
決済機関管理部
144
150
151
相互認証部
暗号化・復号部
KSES

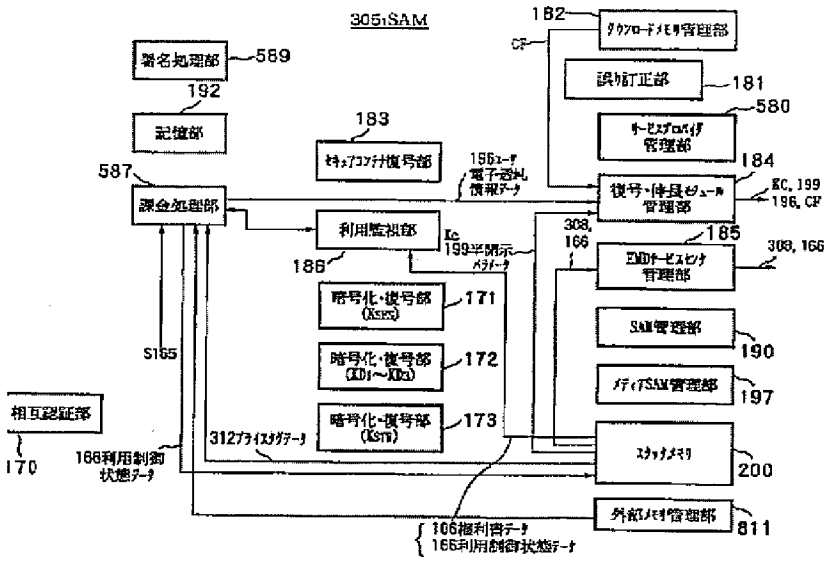
【図７２】


権利書データベース
445a
証明書データベース
445b
証明書・権利書管理部
445
CERSAM1
141
鍵データベース
141a
KD1～KD3
コンテンツID作成部
851
SRP 312プライスタグデータ
KD1～KD3, SIGKD1, ESC～SIGKD3, ESC
149
SAM処理部（通信ゲートウェイ）
SAM1_ID, KSAM1, P, SIG8, SAM1
308
利用履歴データ
CERSAM1, SIG50, ESC
SAMデータベース
149a
決済処理部
442
307c
コンテンツプロバイダ管理部
148
148a
CPデータベース
901
ユーザ嗜好データ生成部
902
マーケティング情報データ生成部
904
マーケティング情報データ
サービスプロバイダ管理部
390
SPデータベース
390a
KF作成部
153
署名処理部
443
相互認証部
150
暗号化・復号部
151
決済機関管理部
91決済機関
152S 決済請求権利データ
152C
152S
152C
144

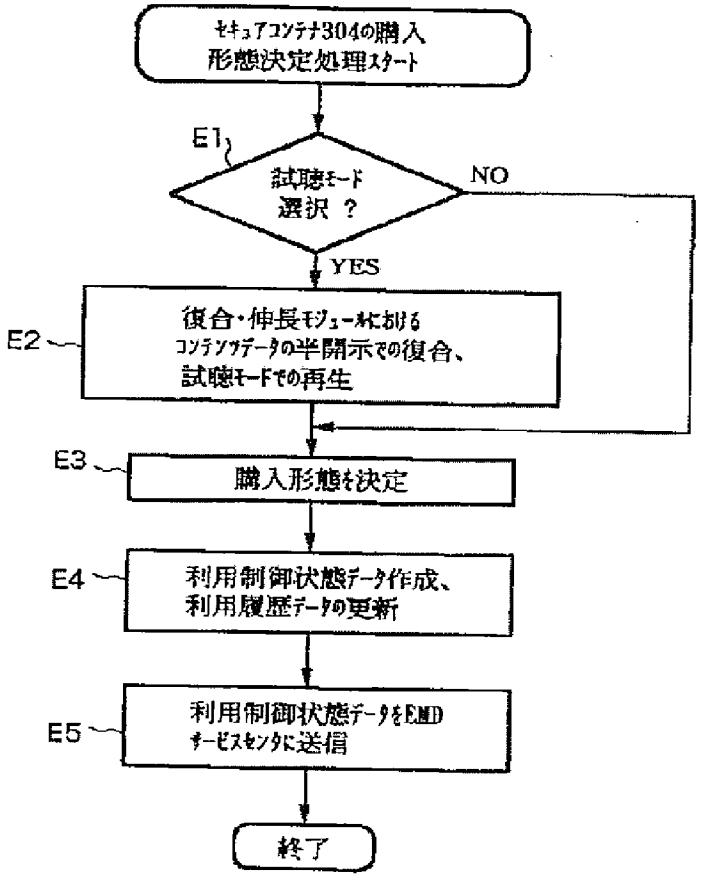
【図７６】


305 SAM
KF
182
ダウンロードメモリ管理部
304
誤り訂正部
181
署名処理部
589
312 プライスタグデータ
192
記憶部
KD1～KD3
183
セキュアコンテナ復号部
サービスプロバイダ管理部
580
903
184
復号・伸長モジュール管理部
186
利用監視部
課金処理部
587
185
EMDサービスセンタ管理部（通信ゲートウェイ）
SAM管理部
KD1～KD3, SIGKD1, ESC～SIGKD3, ESC
903
暗号化・復号部（KSES）
171
CERCP, CRRCP
メディアSAM管理部
190
197
暗号化・復号部（KSTR）
172
CERSP
相互認証部
170
スタックメモリ
200
暗号化・復号部（KSTR, KMED, KFIK）
173
外部メモリ管理部
811

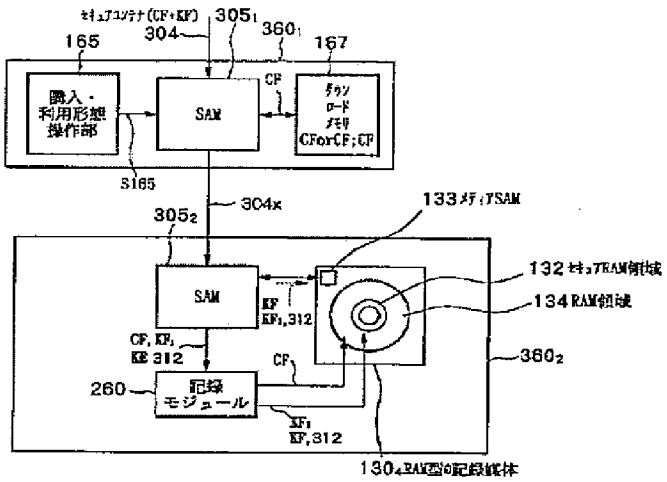
【図７８】


305:SAM
署名処理部
589
192
記憶部
183
セキュアコンテナ復号部
587
課金処理部
利用監視部
186
暗号化・復号部
(Kssm)
171
暗号化・復号部
(KD1～KDn)
172
暗号化・復号部
(KSTB)
173
S165
相互認証部
170
166利用制御
状態データ
312プライスタグデータ
182
ダウンロードメモリ管理部
CF
誤り訂正部
181
580
サービスプロバイダ
管理部
184
復号・伸長モジュール
管理部
Kc, 199
196, CF
155コード
電子透かし
情報データ
Kc
199半開示
パラメータ
308,
166
185
EMDサービスセンタ
管理部
308, 166
SAM管理部
190
メディアSAM管理部
197
スタックメモリ
200
外部メモリ管理部
811
166権利書データ
166利用制御状態データ

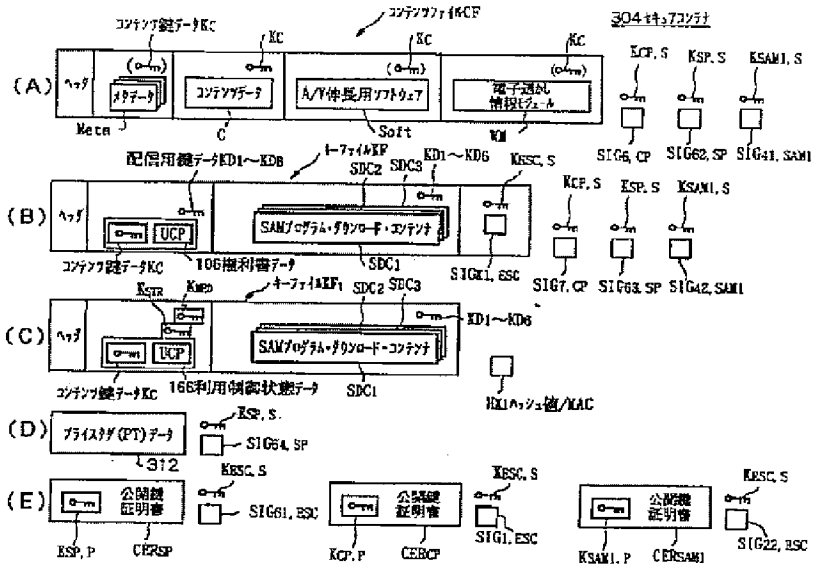
【図７９】


セキュアコンテナ304の購入
形態決定処理スタート
E1
試聴モード
選択 ？
NO
YES
E2
復合・伸長モジュールにおける
コンテンツデータの半開示での復合、
試聴モードでの再生
E3
購入形態を決定
E4
利用制御状態データ作成、
利用履歴データの更新
E5
利用制御状態データをEMD
サービスセンタに送信
終了

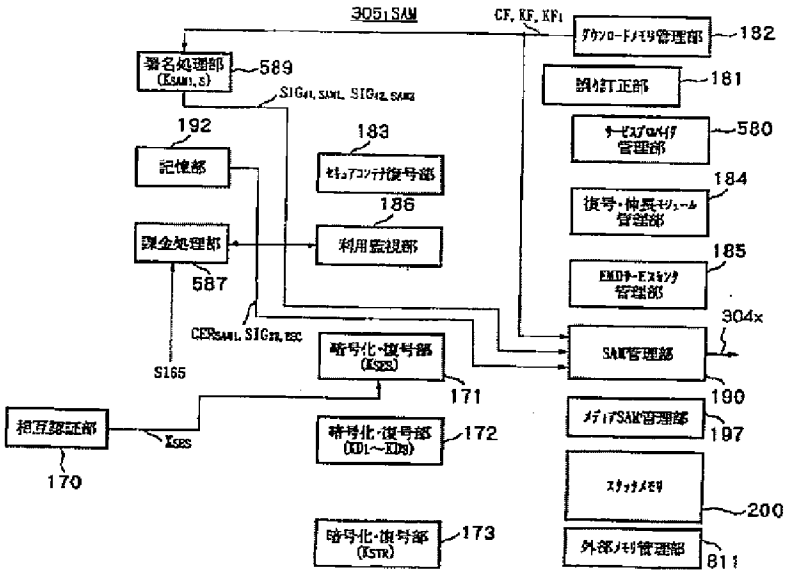
【図８０】


165
304
305₁
360₁
167
購入・利用形態操作部
SAM
CP
ダウンロードメモリ CForCF;CP
S165
304x
305₂
133メディアSAM
SAM
KF KF₁,312
132セキュアRAM領域
134 RAM領域
CF, KF₁ KF 312
CF
360₂
260
記録モジュール
KF₁ KF,312
130₄RAM型の記録媒体

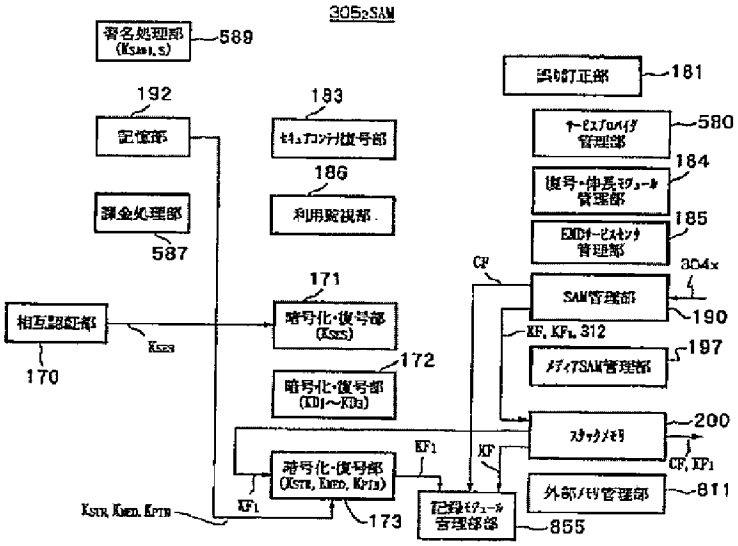
【図８１】


(A)
(B)
(C)
(D)
(E)
KC
KCP, S
KSP, S
KSAM1, S
Meta
C
Soft
SIG6, CP
SIG62, SP
SIG41, SAM1
KD1～KD6
KESC, S
SIG1, ESC
SIG7, CP
SIG63, SP
SIG42, SAM1
UCP
SDC1
SDC2
SDC3
312
SIG64, SP
SIG61, ESC
SIG22, ESC
KSP, P
KCP, P
KSAM1, P

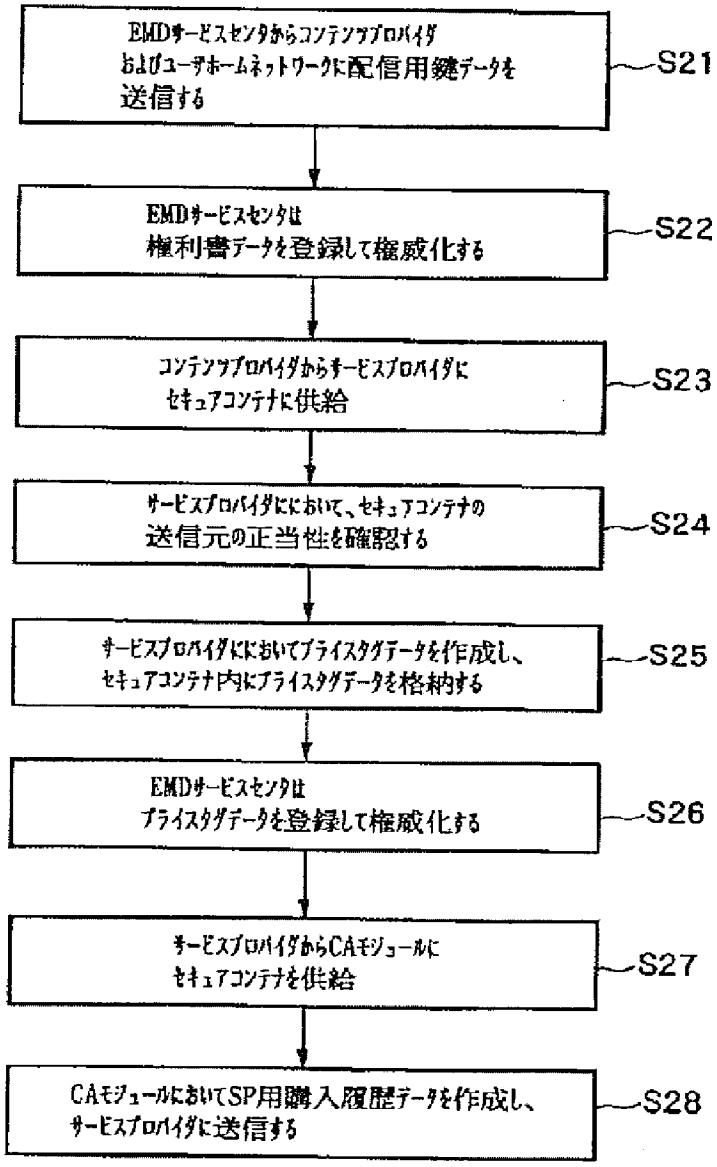
【図８２】


305₁SAM
CF, KF, KF1
ダウンロードメモリ管理部
182
署名処理部
(KSAM1, S)
589
SIG#1, SAM1, SIG#2, SAM2
時計訂正部
181
192
183
サービスプロバイダ管理部
580
記憶部
セキュアコンテナ復号部
186
184
復号・伸長モジュール管理部
課金処理部
利用監視部
185
587
EMDサービスセンタ管理部
304x
CERSAM1, SIGSI, ESC
暗号化・復号部
(KSES)
SAM管理部
S165
171
190
メディアSAM管理部
197
相互認証部
KSES
暗号化・復号部
(KD1～KDn)
172
170
スタックメモリ
200
暗号化・復号部
(KSTR)
173
外部メモリ管理部
811

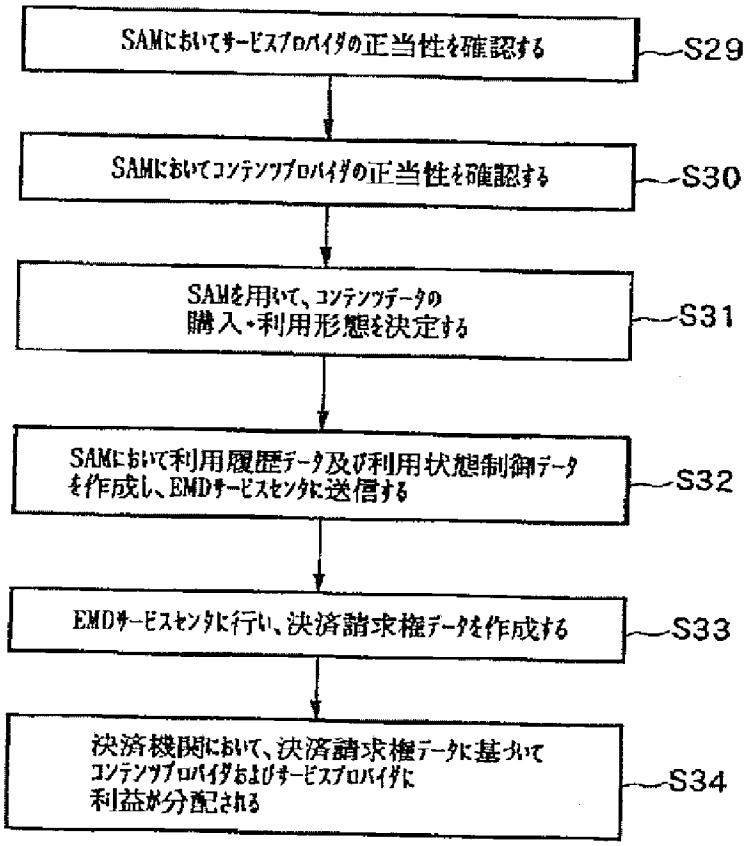
【図８３】


305₂SAM
署名処理部
(KSAM1, S)
589
時計訂正部
181
192
183
記憶部
セキュアコンテナ復号部
サービスプロバイダ管理部
580
186
184
利用監視部
復号・伸長モジュール管理部
課金処理部
587
185
EMDサービスセンタ管理部
CF
304x
171
SAM管理部
相互認証部
暗号化・復号部
(KSES)
190
KSES
KF, KF1, 312
197
170
172
メディアSAM管理部
暗号化・復号部
(KD1～KDn)
200
スタックメモリ
KF1
KF
暗号化・復号部
(KSTR, KMED, KPTB)
CF, KF1
KF1
外部メモリ管理部
811
KSTR, KMED, KPTB
173
記録モジュール管理部
855

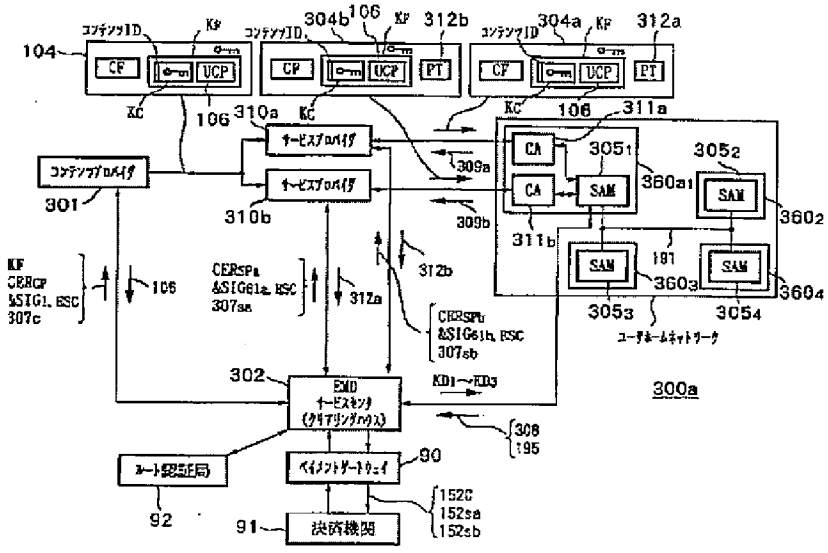
【図８４】


EMDサービスセンタからコンテンツプロバイダおよびユーザホームネットワークに配信用鍵データを送信する
S21
EMDサービスセンタは権利書データを登録して権威化する
S22
コンテンツプロバイダからサービスプロバイダにセキュアコンテナに供給
S23
サービスプロバイダにおいて、セキュアコンテナの送信元の正当性を確認する
S24
サービスプロバイダにおいてプライスタグデータを作成し、セキュアコンテナ内にプライスタグデータを格納する
S25
EMDサービスセンタはプライスタグデータを登録して権威化する
S26
サービスプロバイダからCAモジュールにセキュアコンテナを供給
S27
CAモジュールにおいてSP用購入履歴データを作成し、サービスプロバイダに送信する
S28

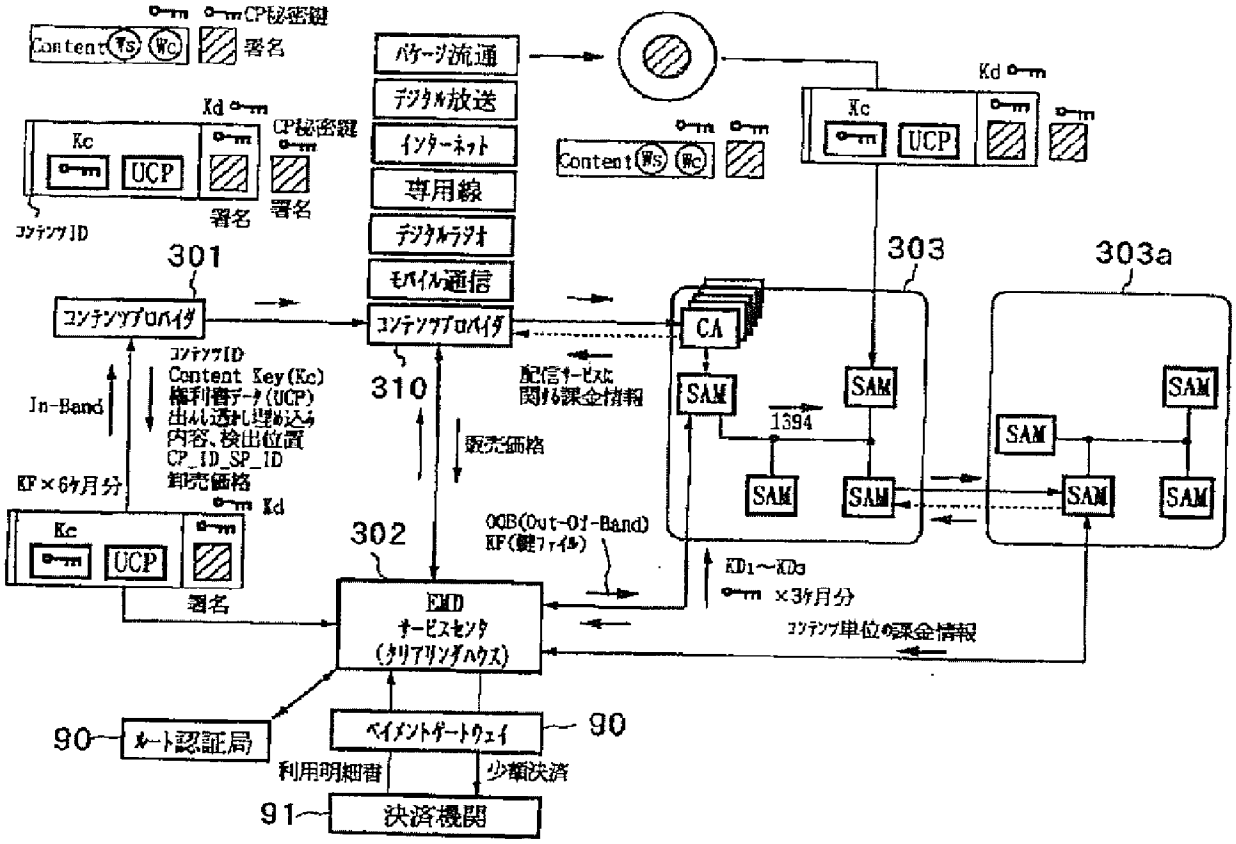
【図８５】


SAMにおいてサービスプロバイダの正当性を確認する
S29
SAMにおいてコンテンツプロバイダの正当性を確認する
S30
SAMを用いて、コンテンツデータの
購入・利用形態を決定する
S31
SAMにおいて利用履歴データ及び利用状態制御データ
を作成し、EMDサービスセンタに送信する
S32
EMDサービスセンタに行い、決済請求権データを作成する
S33
決済機関において、決済請求権データに基づいて
コンテンツプロバイダおよびサービスプロバイダに
利益が分配される
S34

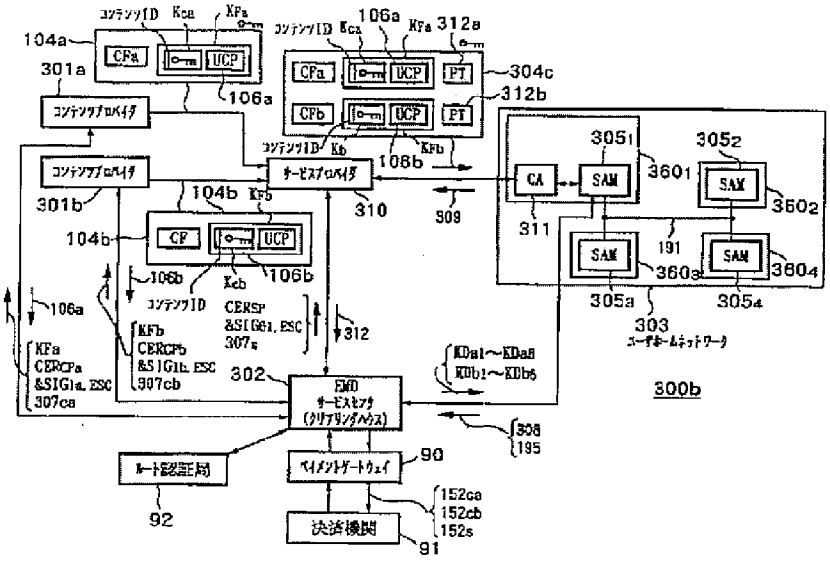
【図９７】


104
CF
UCP
PT
KC
106
310a
310b
309a
309b
311a
311b
コンテンツプロバイダ
301
サービスプロバイダ
CA
SAM
305₁
305₂
305₃
305₄
360a₁
360₂
360₃
360₄
197
312a
312b
304a
304b
KF
CERCP
&SIG1, RSC
307c
CERSPa
&SIG61a, RSC
307sa
CERSPb
&SIG61b, RSC
307sb
312a
KD1～KD3
300a
302
EMD
サービスセンタ
308
195
90
92
91
決済機関
152c
152sa
152sb

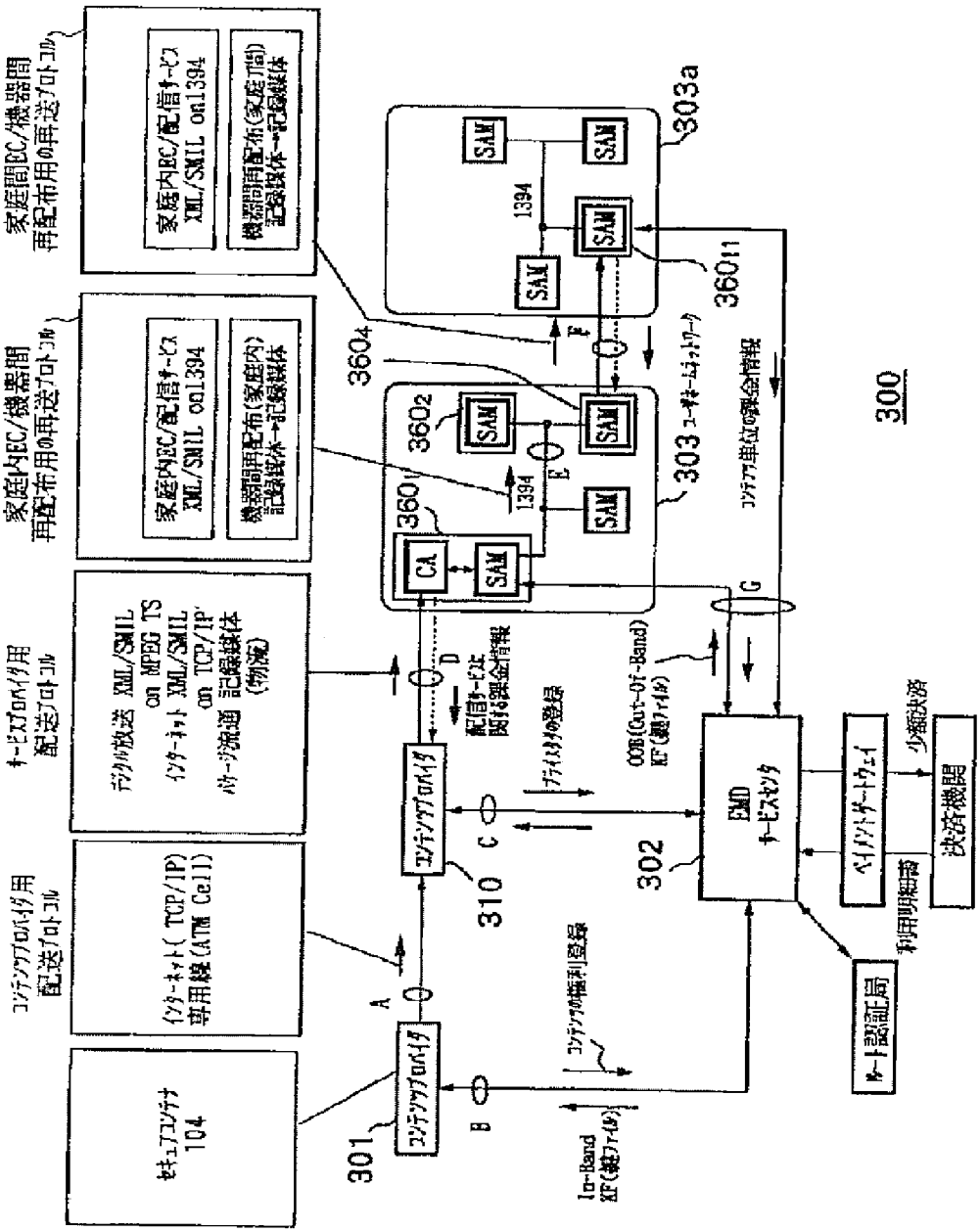
【図８６】


CP秘密鍵
署名
Content
Ws
Wc
パッケージ流通
デジタル放送
インターネット
専用線
デジタルラジオ
モバイル通信
Kd
Kc
UCP
CP秘密鍵
署名
コンテンツID
301
303
303a
コンテンツプロバイダ
310
CA
SAM
1394
In-Band
コンテンツID
Content Key(Kc)
権利者データ(UCP)
出かし透かし埋め込み
内容、検出位置
CP_ID_SP_ID
販売価格
配信サービスに
関わる課金情報
KF×6ヶ月分
販売価格
302
OOB(Out-Of-Band)
KF(鍵ファイル)
KD1～KDn
×3ヶ月分
コンテンツ単位の課金情報
EMD
サービスセンタ
(クリアリングハウス)
90
ルート認証局
ペイメントゲートウェイ
利用明細書
少額決済
91
決済機関

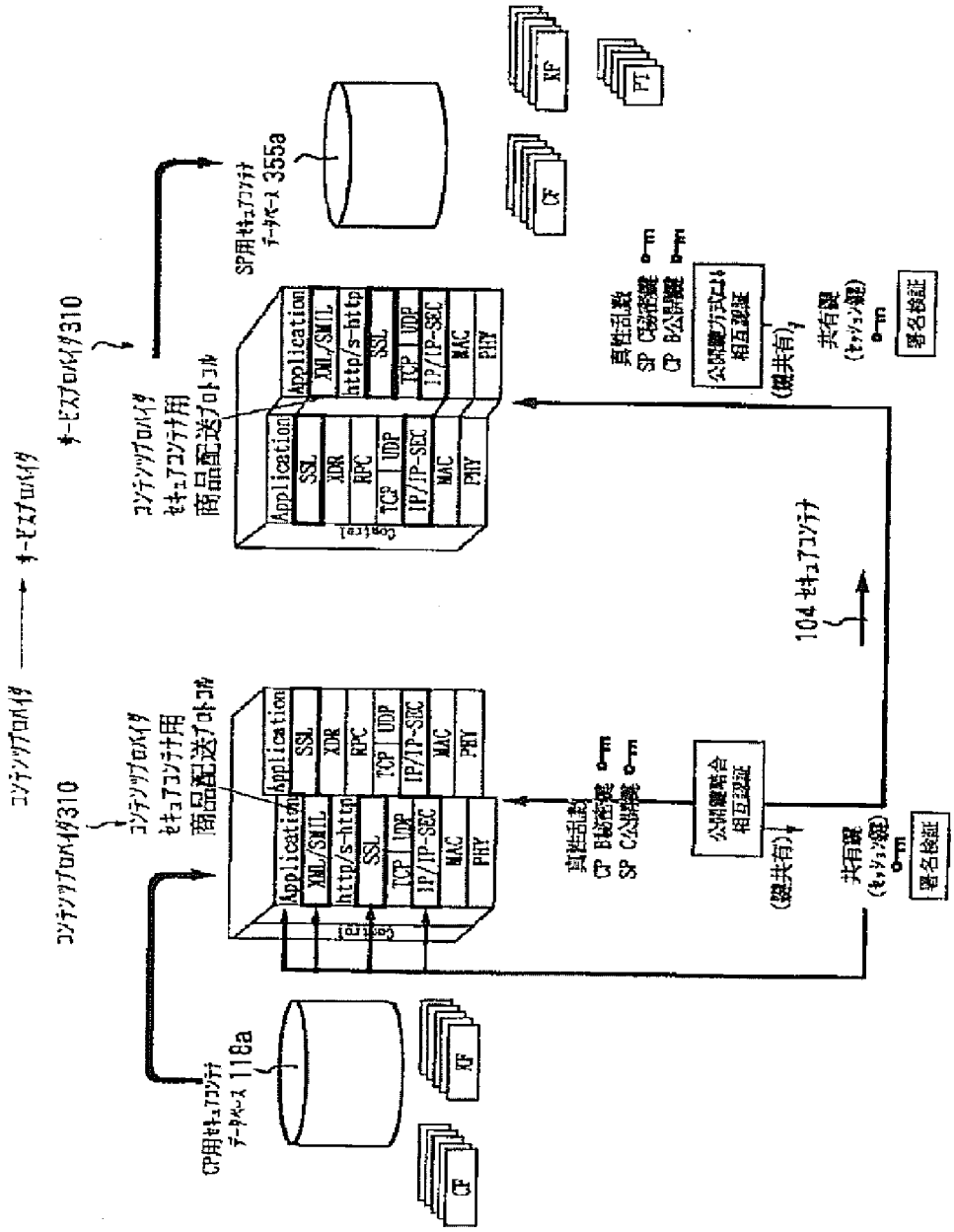
【図９８】


104a
301a
CPa
UCP
106a
コンテンツプロバイダ
106a
Kca
KFa
312a
CPb
PT
304c
312b
301b
サービスプロバイダ
106b
KFb
Kb
104b
CP
310
309
CA
SAM
3051
3601
305a
3602
305b
3603
305a
3604
305a
311
191
303
ユーザホームネットワーク
300b
CERSP
&SIGb, ESC
307a
312
KFa
CERCPa
&SIGa, ESC
307ca
KFb
CERCPb
&SIGb, ESC
307cb
302
EMD
サービスセンタ
(クリアリングハウス)
KDa1～KDan
KDb1～KDbn
308
195
ルート認証局
92
ペイメントゲートウェイ
90
決済機関
91
152ca
152cb
152s

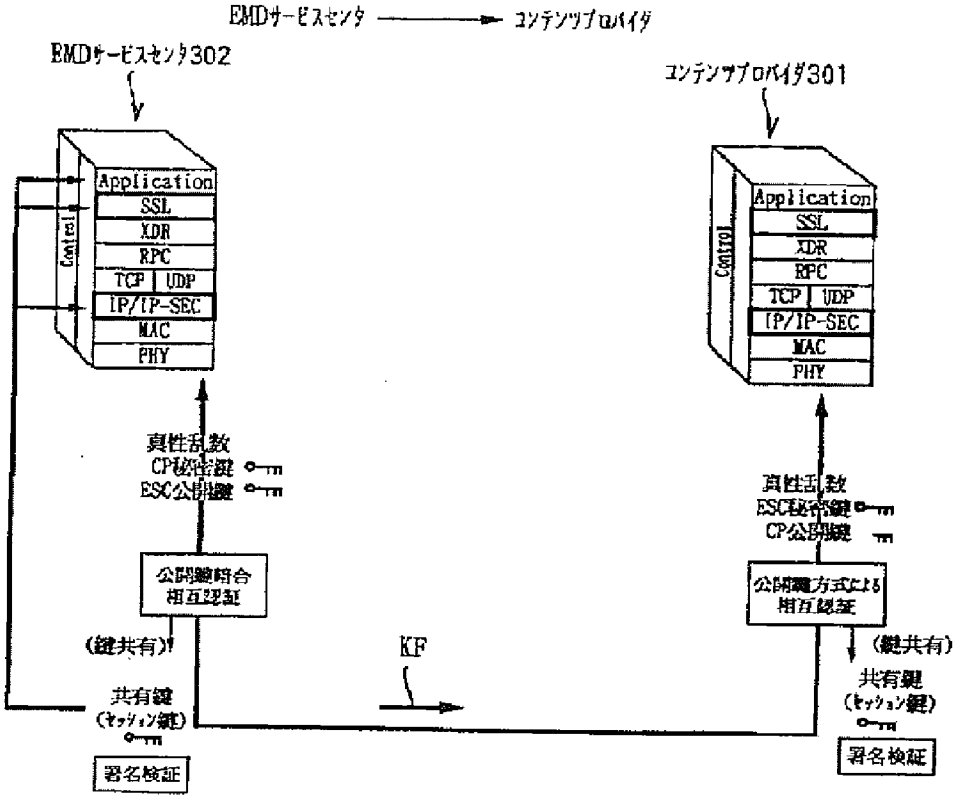
【図８７】


家庭間EC/機器間
再配布用の再送プロトコル
家庭内EC/機器間
再配布用の再送プロトコル
サービスプロバイダ用
配送プロトコル
コンテンツプロバイダ用
配送プロトコル
家庭内EC/配信サービス
XML/SMIL on1394
機器間再配布(家庭間)
記録媒体→記録媒体
家庭内EC/配信サービス
XML/SMIL on1394
機器間再配布(家庭内)
記録媒体→記録媒体
デジタル放送 XML/SMIL
on MPEG TS
インターネット XML/SMIL
on TCP/IP
パッケージ流通 記録媒体
(物流)
インターネット(TCP/IP)
専用線(ATM Cell)
セキュアコンテナ
104
301
310
302
303
303a
300
3601
3602
3604
3611
SAM
CA
1394
EMD
サービスセンタ
ペイメントゲートウェイ
決済機関
ユーザ認証局
利用明細書
配信サービス
関連課金情報
デバイスの登録
コンテンツの権利登録
In-Band
IP(通信パス)
OOB(Out-Of-Band)
IP(通信パス)
コンテンツ単位の課金情報
A
B
C
D
E
F
G

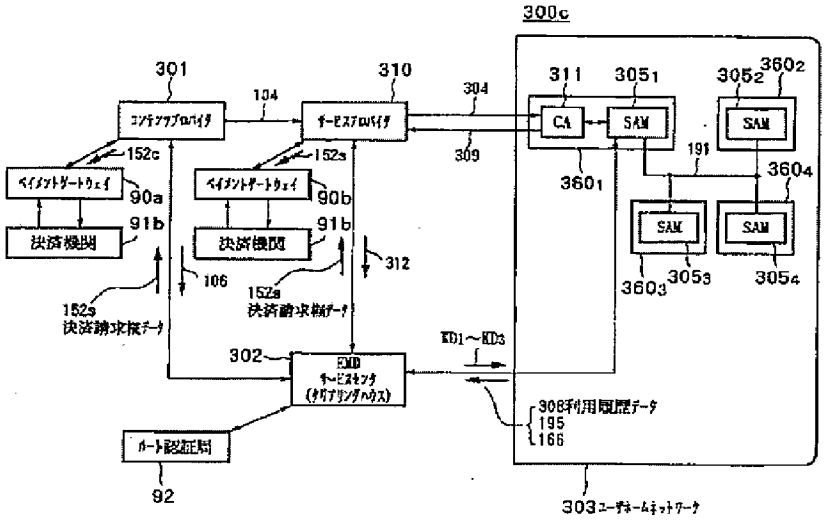
【図８８】


コンテンツプロバイダ310
サービスプロバイダ
コンテンツプロバイダ
セキュアコンテナ用
商品配送プロトコル
SP用セキュアコンテナ
データベース 355a
Application
XML/SMIL
http/s-http
SSL
TCP UDP
IP/IP-SEC
MAC
PHY
KF
PT
CF
真性乱数
SP C秘密鍵
CP B公開鍵
公開鍵方式による
相互認証
(鍵共有)
共有鍵
(セッション鍵)
署名検証
104 セキュアコンテナ
コンテンツプロバイダ310
コンテンツプロバイダ
セキュアコンテナ用
商品配送プロトコル
CP用セキュアコンテナ
データベース 118a
真性乱数
CP B秘密鍵
SP C公開鍵
公開鍵方式による
相互認証
(鍵共有)
共有鍵
(セッション鍵)
署名検証

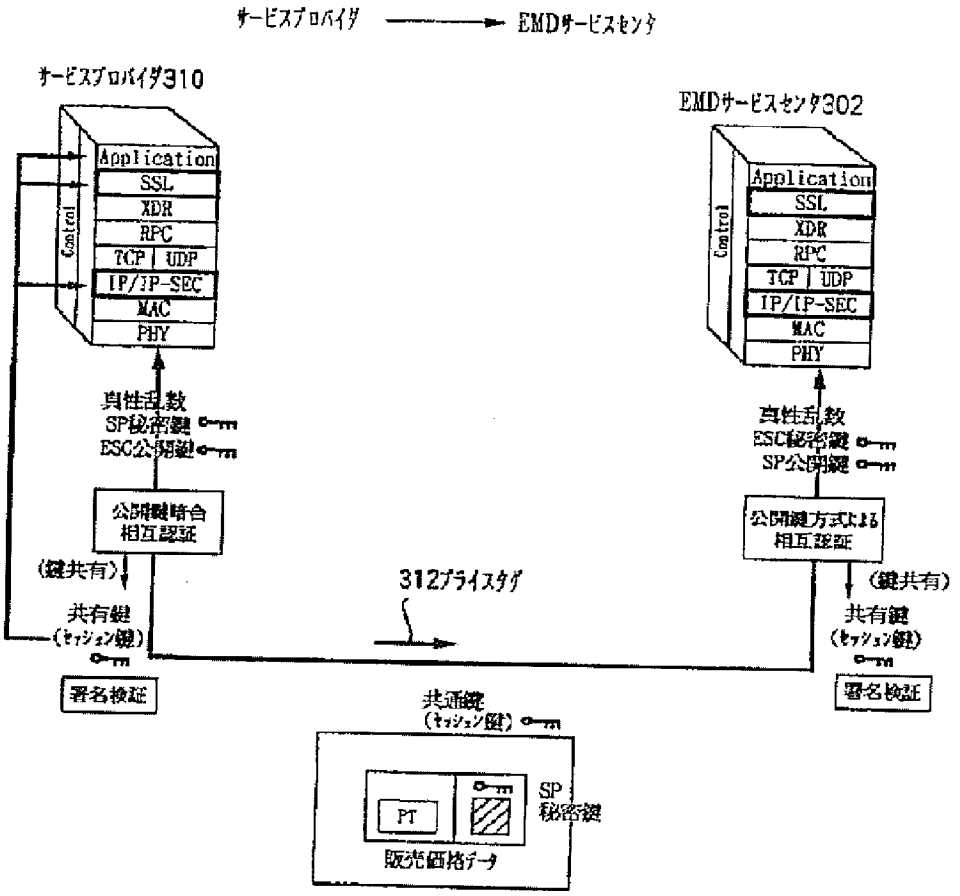
【図８９】


EMDサービスセンタ
コンテンツプロバイダ
EMDサービスセンタ302
コンテンツプロバイダ301
Application
SSL
XDR
RPC
TCP
UDP
IP/IP-SEC
MAC
PHY
Control
真性乱数
CP秘密鍵
ESC公開鍵
公開鍵暗号相互認証
(鍵共有)
共有鍵
(セッション鍵)
署名検証
KF
真性乱数
ESC秘密鍵
CP公開鍵
公開鍵方式による相互認証
(鍵共有)
共有鍵
(セッション鍵)
署名検証

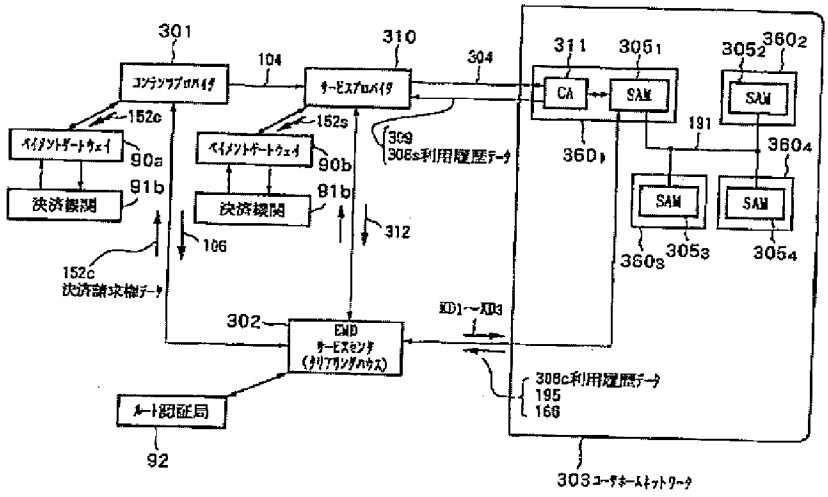
【図９９】


300c
301
310
311
3051
3052
3602
304
309
3601
191
3604
3603
3053
3054
CA
SAM
152c
152a
90a
90b
91b
91b
312
106
152a
302
KD1～KD3
92
303
195
196

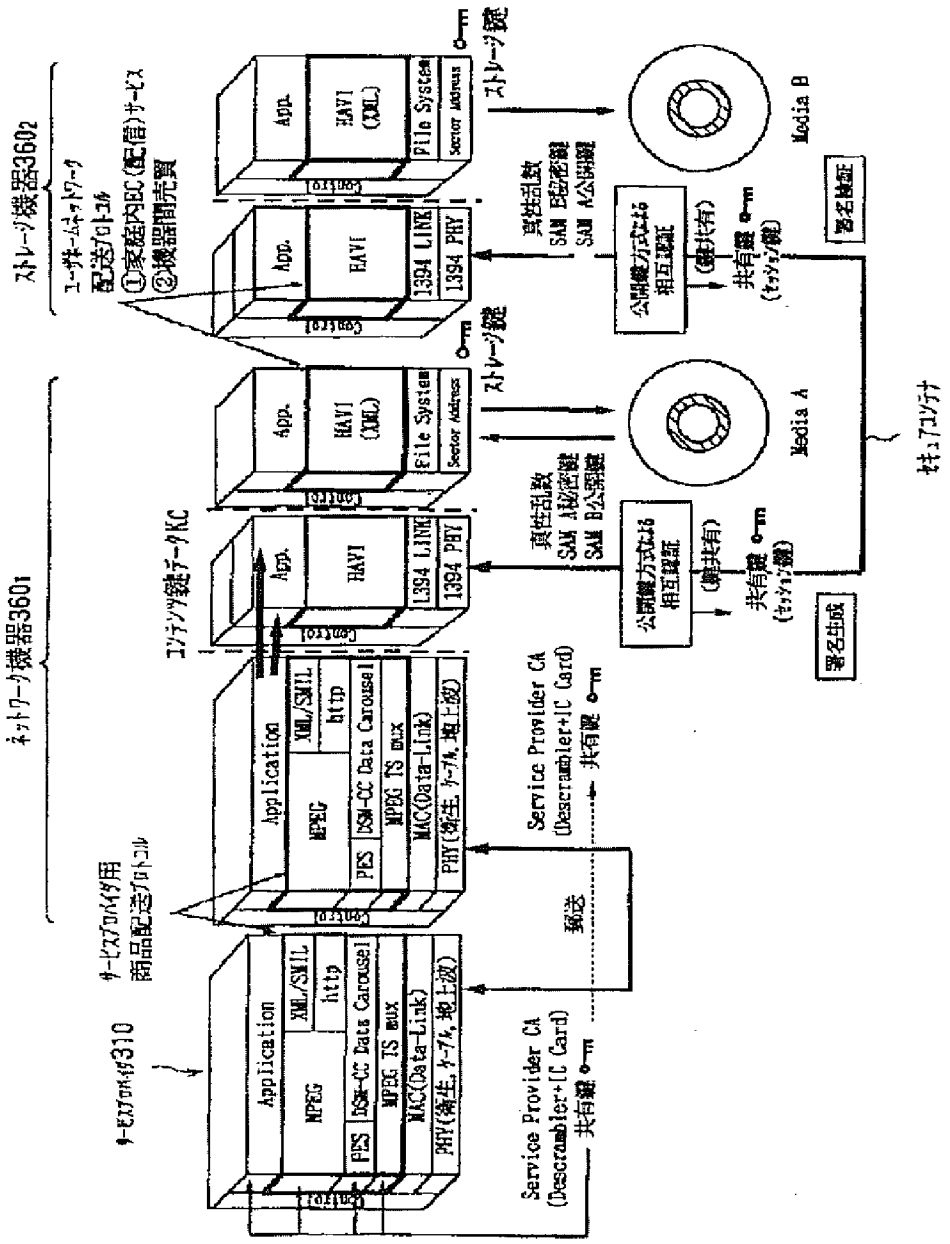
【図９０】


サービスプロバイダ
EMDサービスセンタ
サービスプロバイダ310
EMDサービスセンタ302
Application
SSL
XDR
RPC
TCP | UDP
IP/IP-SEC
MAC
PHY
Control
真性乱数
SP秘密鍵
ESC公開鍵
公開鍵暗合相互認証
(鍵共有)
共有鍵
(セッション鍵)
署名検証
312プライスタグ
真性乱数
ESC秘密鍵
SP公開鍵
公開鍵方式による相互認証
(鍵共有)
共有鍵
(セッション鍵)
署名検証
共通鍵
(セッション鍵)
PT
SP秘密鍵
販売価格データ

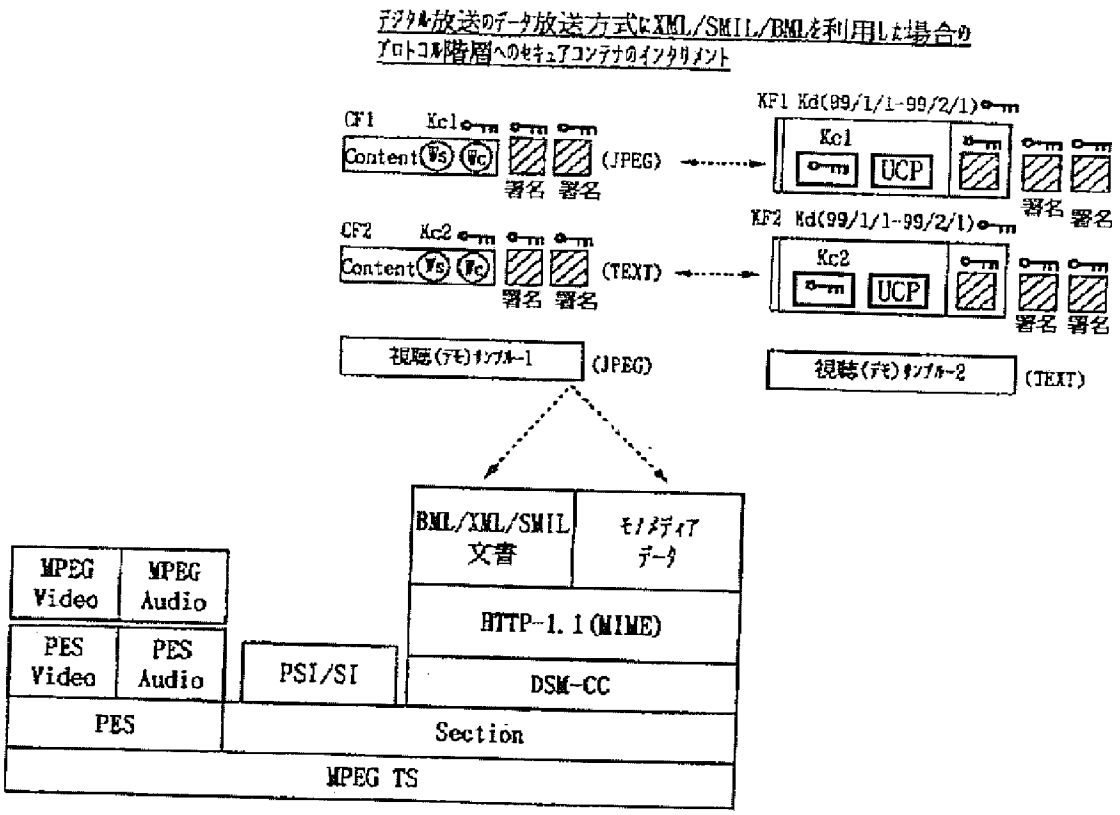
【図１００】


301
310
104
304
311
305₁
305₂
360₂
CA
SAM
SAM
152a
152s
309
308s利用履歴データ
191
360₄
90a
90b
360D
91b
91b
SAM
SAM
決済機関
決済機関
312
106
360₃
305₃
305₄
152c
決済請求権データ
302
XD1～XDn
EMD
サービスセンタ
(クリアリングハウス)
308c利用履歴データ
195
160
ルート認証局
92
303ユーザホームネットワーク

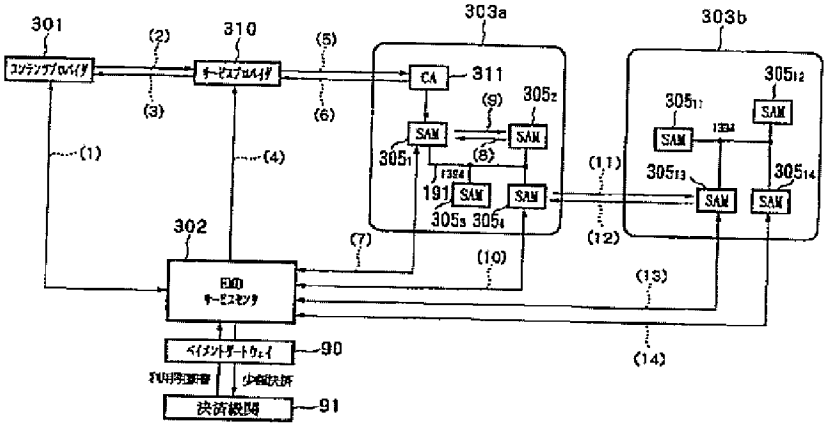
【図９１】


ストレージ機器3602
ユーザホームネットワーク
配送プロトコル
①家庭内EC(配信)サービス
②機器間売買
ネットワーク機器3601
サービスプロバイダ用
商品配送プロトコル
エンティティ鍵データKC
ストレージ鍵
ストレージ鍵
Media B
Media A
App.
HAVi
(XML)
File System
Sector Address
HAVi
1394 LINK
1394 PHY
Application
XML/SMIL
http
MPEG
PES
DSM-CC Data Carousel
MPEG TS mux
MAC(Data-Link)
PHY(変調, ケーブル, 地上波)
Service Provider CA
(Descrambler+IC Card)
共有鍵
配送
真性乱数
SAM A秘密鍵
SAM B公開鍵
公開鍵方式による
相互認証
(鍵共有)
共有鍵
(セッション鍵)
署名生成
署名検証
ネットワーク

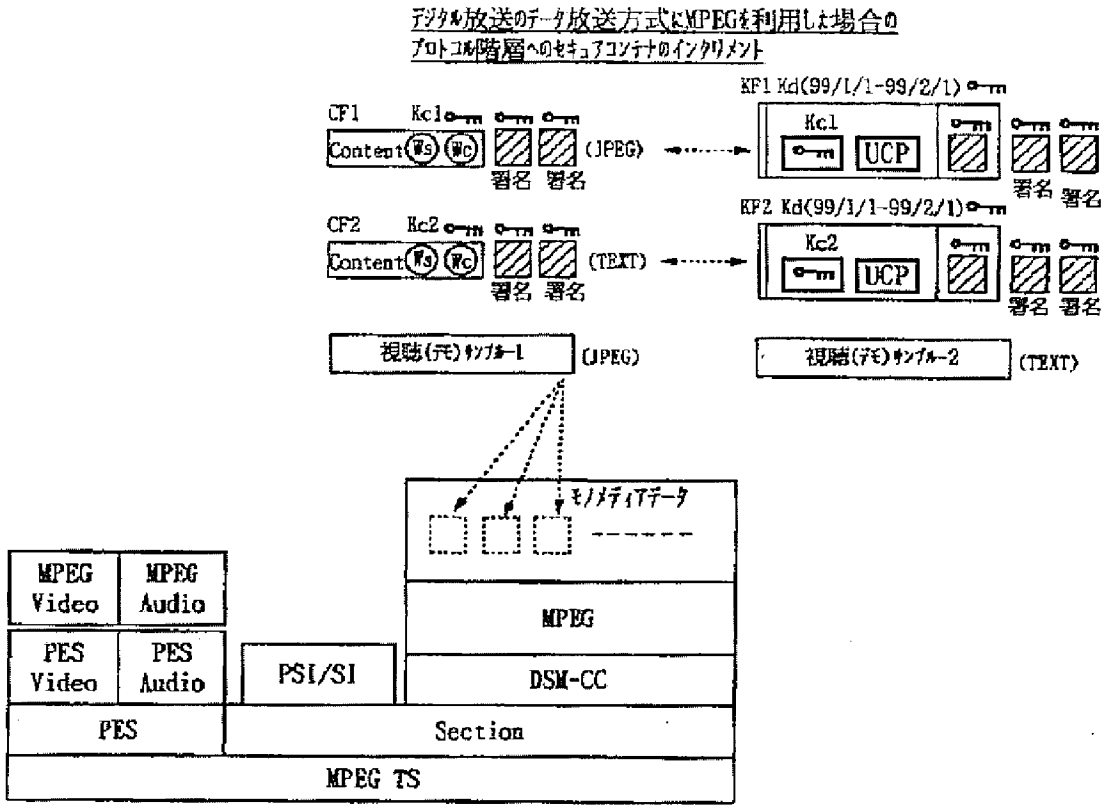
【図９２】


デジタル放送のデータ放送方式にXML/SMIL/BMLを利用した場合の
プロトコル階層へのセキュアコンテナのインクリメント
CF1
Kc1
Content
Vs
Vc
(JPEG)
署名
署名
KF1 Kd(99/1/1-99/2/1)
Kc1
UCP
署名
署名
CF2
Kc2
Content
Vs
Vc
(TEXT)
署名
署名
KF2 Kd(99/1/1-99/2/1)
Kc2
UCP
署名
署名
視聴(デモ)サンプル-1
(JPEG)
視聴(デモ)サンプル-2
(TEXT)
BML/XML/SMIL
文書
モノメディア
データ
MPEG
Video
MPEG
Audio
HTTP-1.1(MIME)
PES
Video
PES
Audio
PSI/SI
DSM-CC
PES
Section
MPEG TS

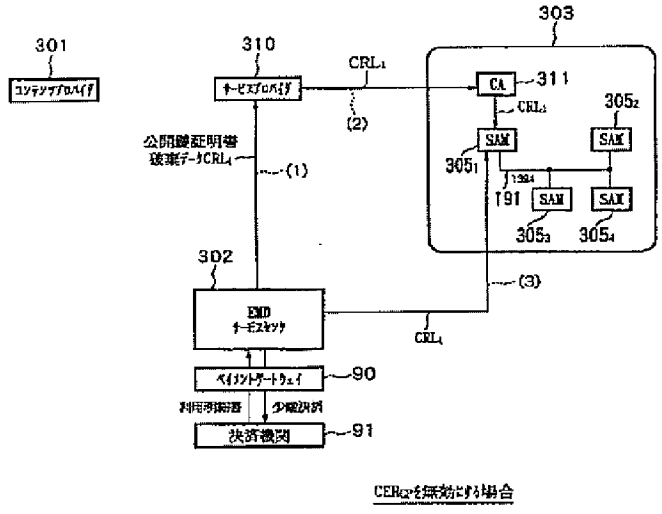
【図１０１】


301
(2)
310
(5)
303a
303b
CA
311
(9)
305₂
SAM
(8)
305₁
1394
191
305₃
305₄
(1)
(4)
(3)
(6)
(11)
(12)
305₁₁
305₁₂
305₁₃
305₁₄
302
(7)
(10)
(13)
(14)
90
91
公開鍵証明書の入手ルート

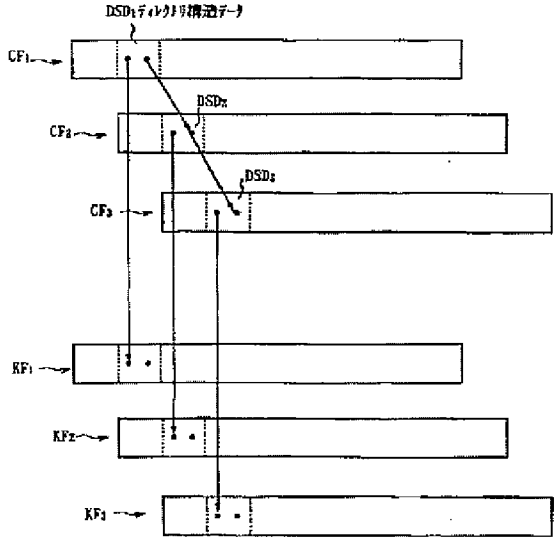
【図９３】



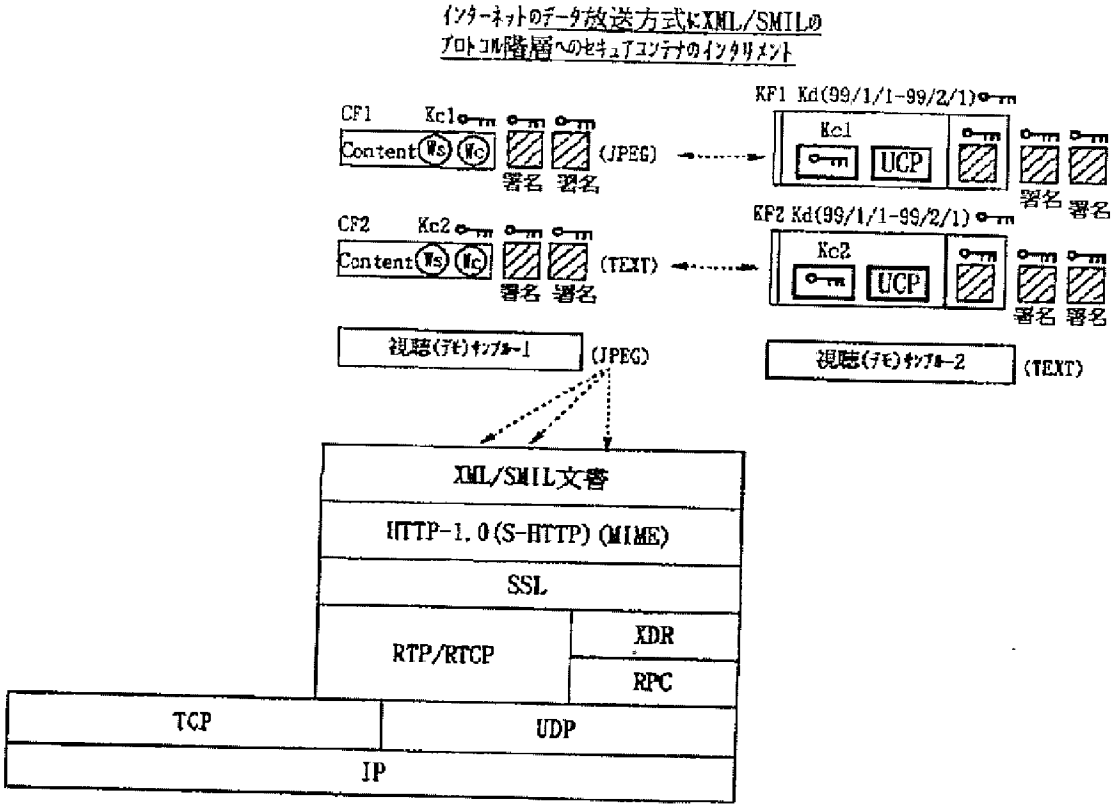
【図１０２】



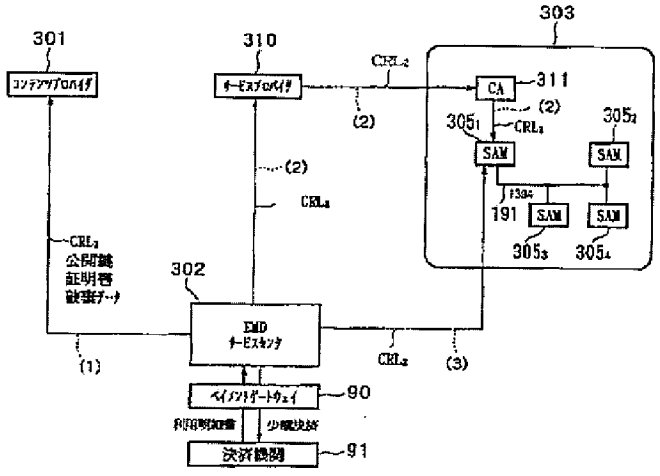
【図１１２】



【図９４】

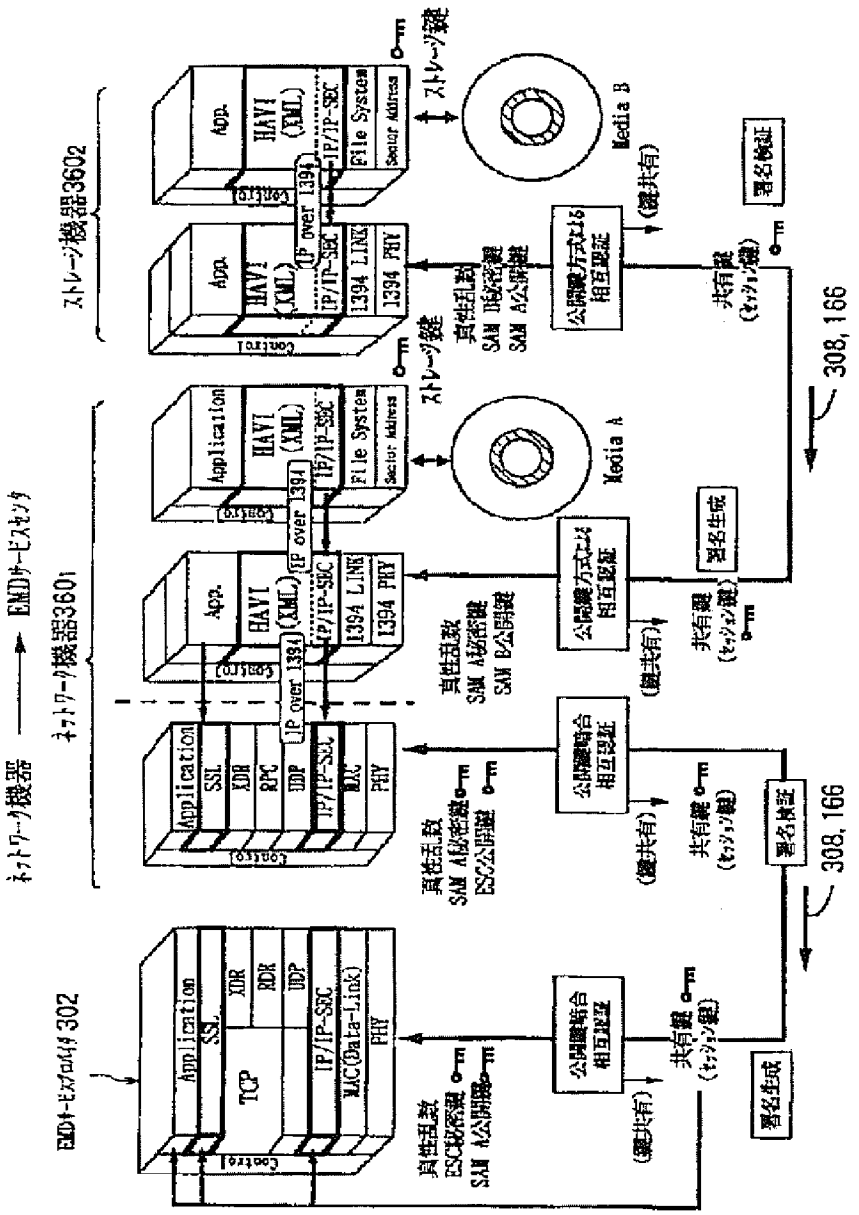


【図１０３】

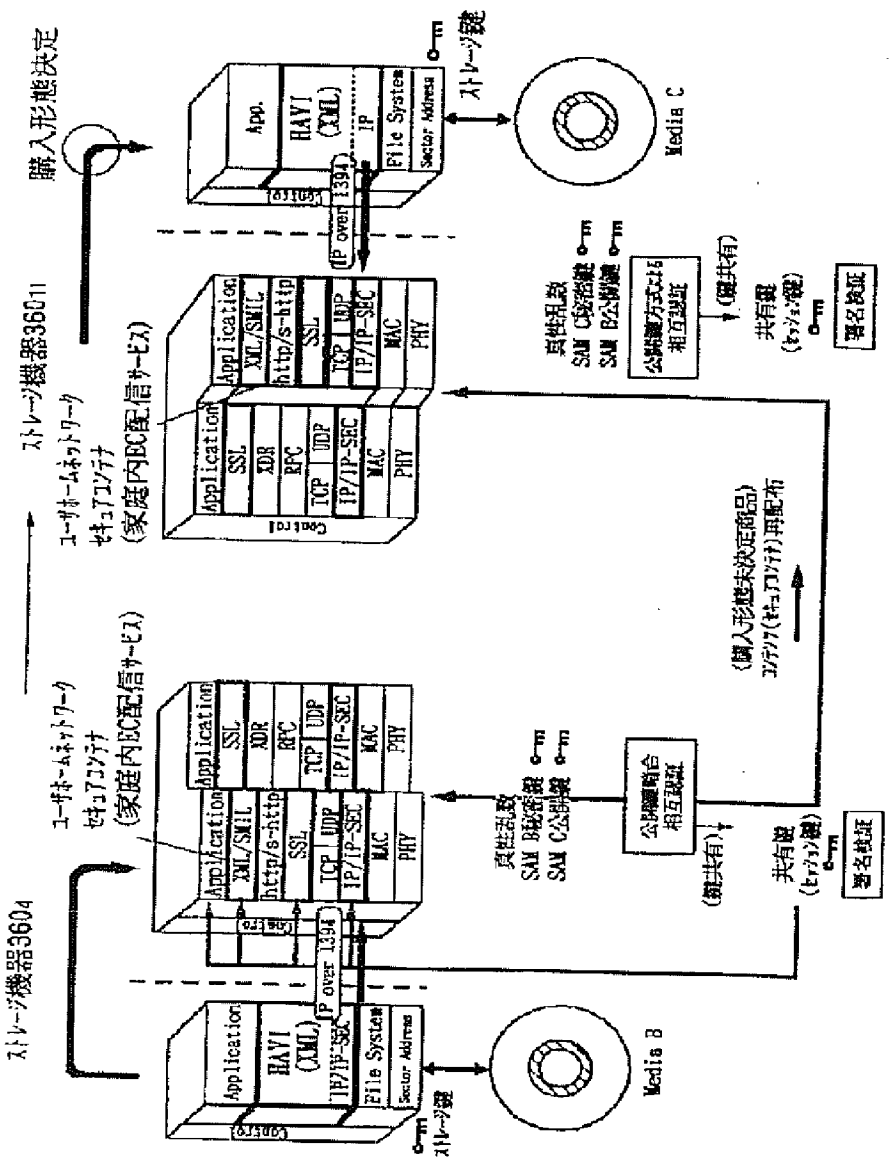


CERTを無効とする場合

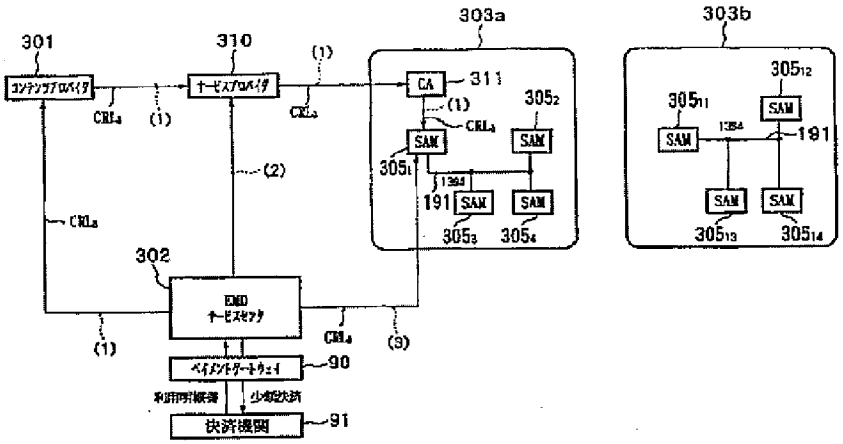
【図９５】


ネットワーク機器
EMDサービスセンタ
ネットワーク機器3601
ストレージ機器3602
EMDサービスセンタ302
Application
SSL
XDR
RDR
UDP
TCP
IP/IP-SSC
MAC(Data-Link)
PHY
IP over 1394
1394 LINK
1394 PHY
HAVI (XML)
App.
Control
File System
Sector Address
Media A
Media B
ストレージ鍵
真性乱数
SAM A秘密鍵
SAM B公開鍵
ESC公開鍵
公開鍵方式による相互認証
(鍵共有)
共有鍵 (セッション鍵)
署名生成
署名検証
308, 166

【図９６】

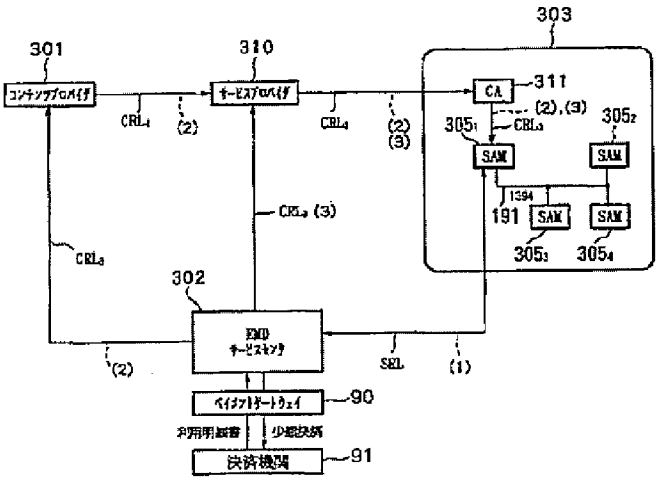

購入形態決定
ストレージ機器3601
ユーザホームネットワーク
セキュアコンテナ
(家庭内BC配信サービス)
ストレージ機器3604
ユーザホームネットワーク
セキュアコンテナ
(家庭内BC配信サービス)
Application
XML/SMIL
http/s-http
SSL
TCP
UDP
IP/IP-SEC
MAC
PHY
ADR
RPC
1394
IP over 1394
HAVI (XML)
IP
File System
Sector Address
ストレージ鍵
Media C
Media B
真性乱数
SAM C秘密鍵
SAM C公開鍵
公開鍵暗号相互認証
(鍵共有)
共有鍵
(セッション鍵)
署名検証
SAM B秘密鍵
SAM B公開鍵
(購入形態未決定商品)
コンテンツ(セキュアコンテナ)再配布

【図１０４】

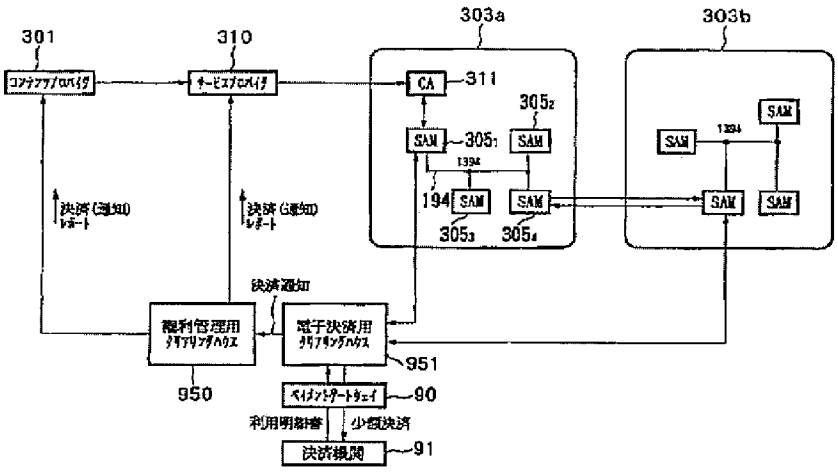


CERSAM2を無効とする場合

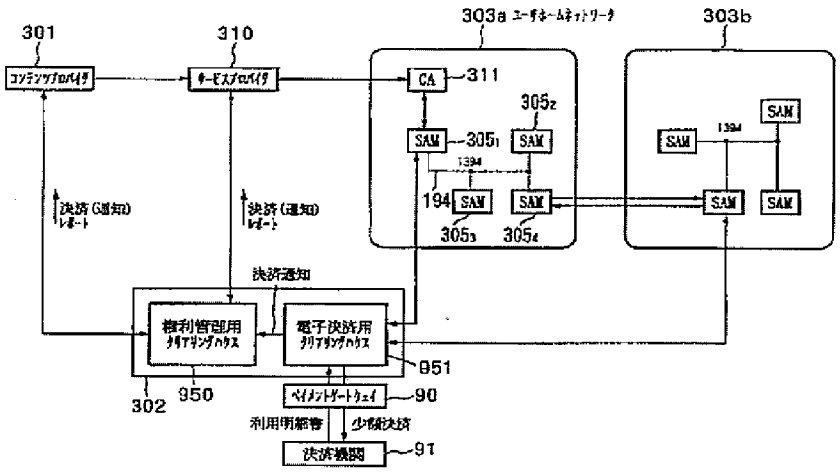
【図１０５】



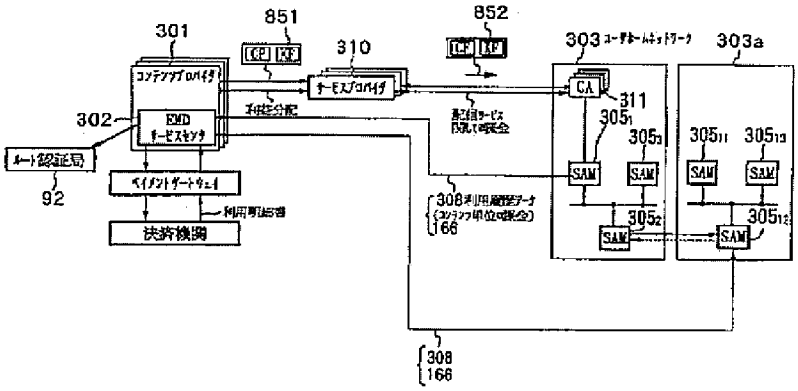
【図１０６】



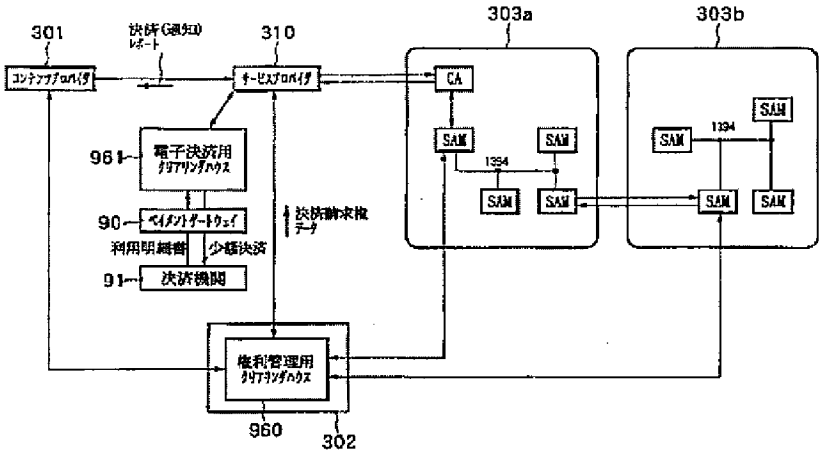
【図１０７】



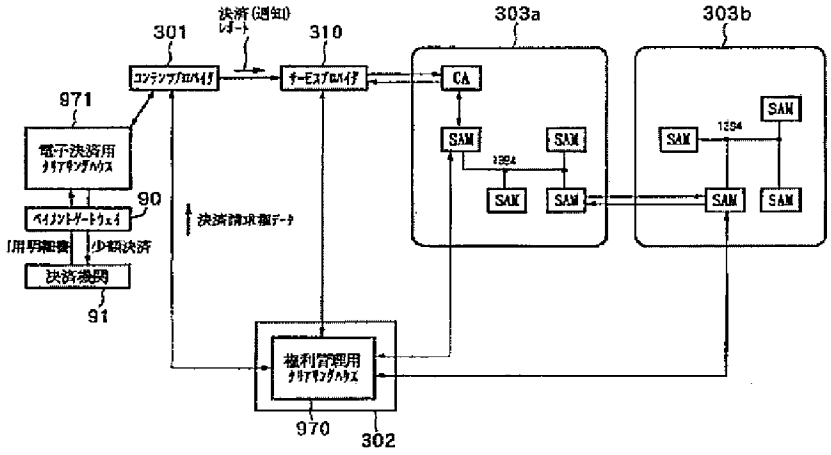
【図１４３】



【図１０８】



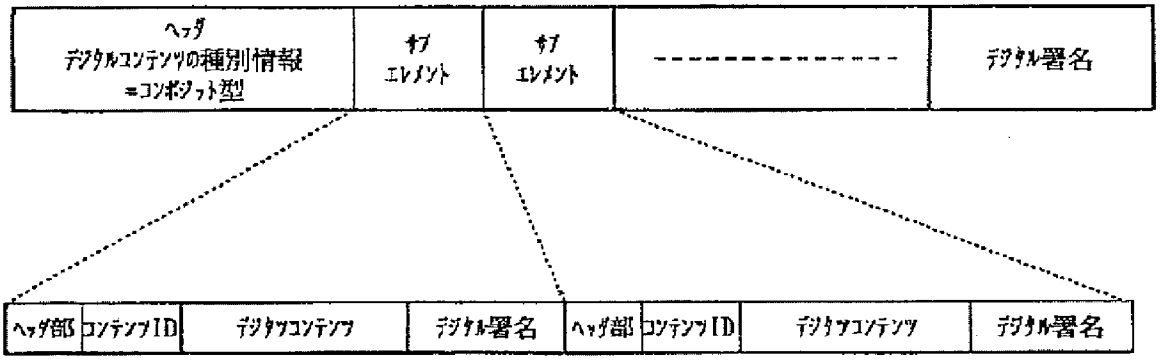
【図１０９】



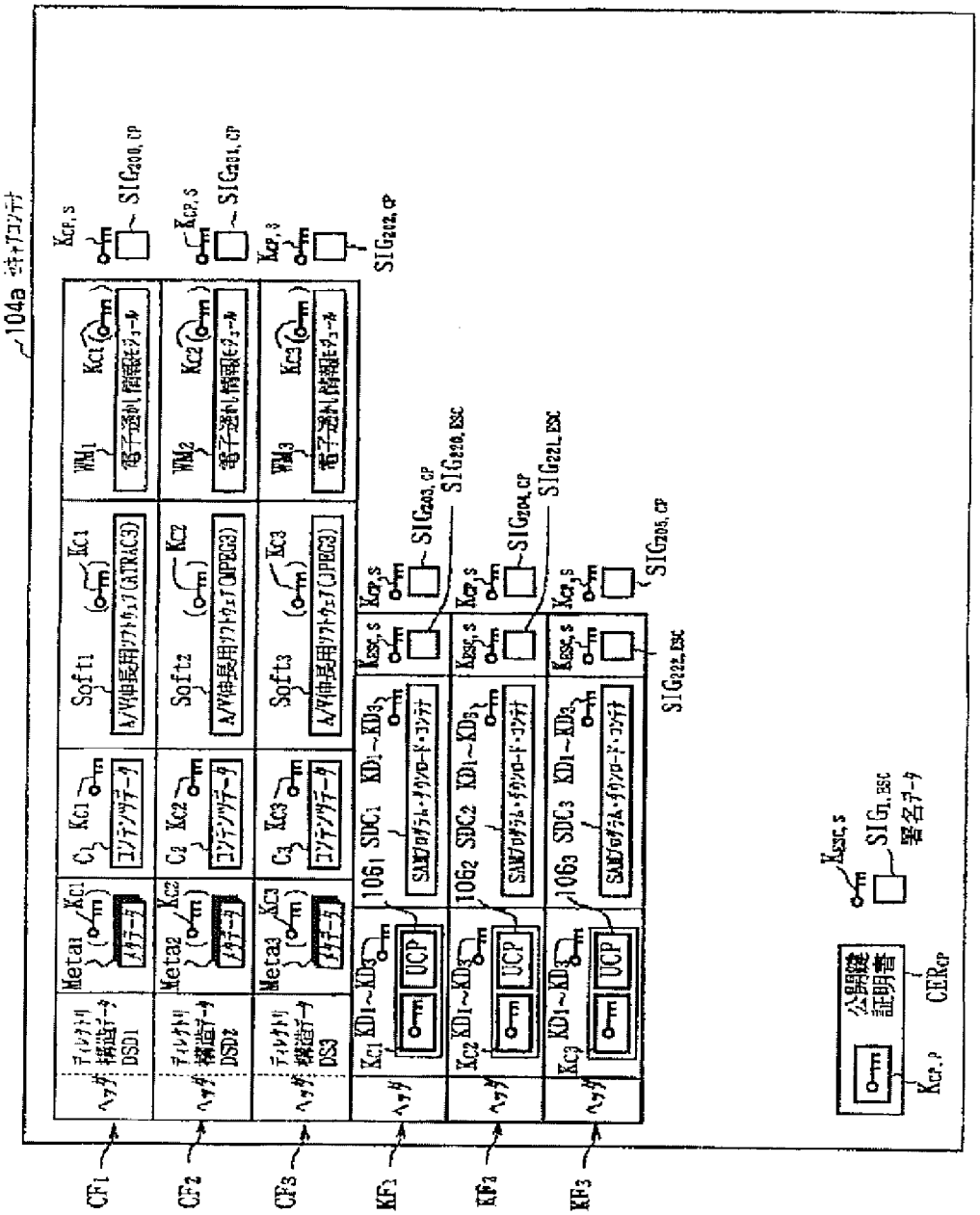
【図１１５】

セキュアコンテナ（コンポジット型）のデータフォーマット－①

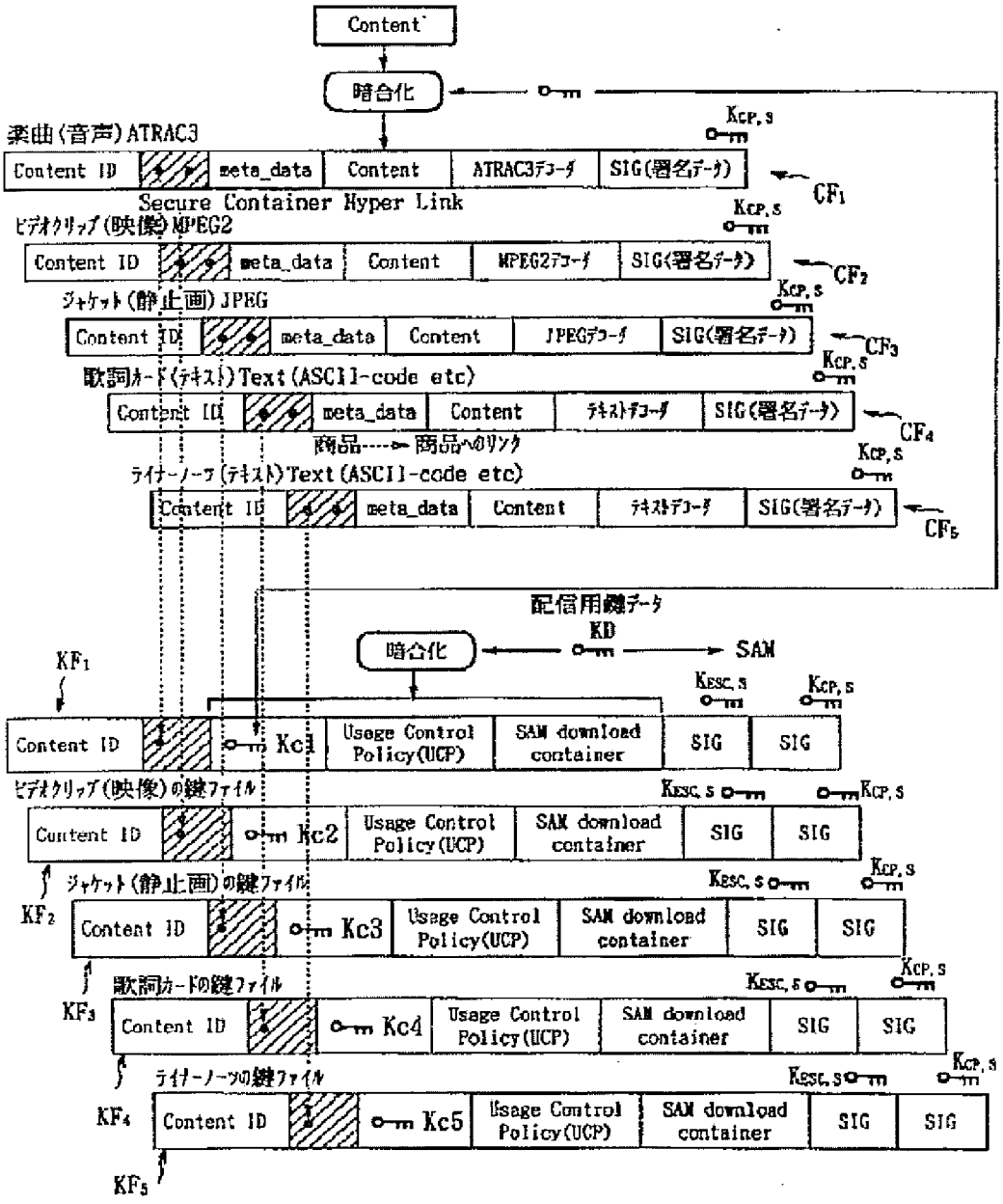
基本構成



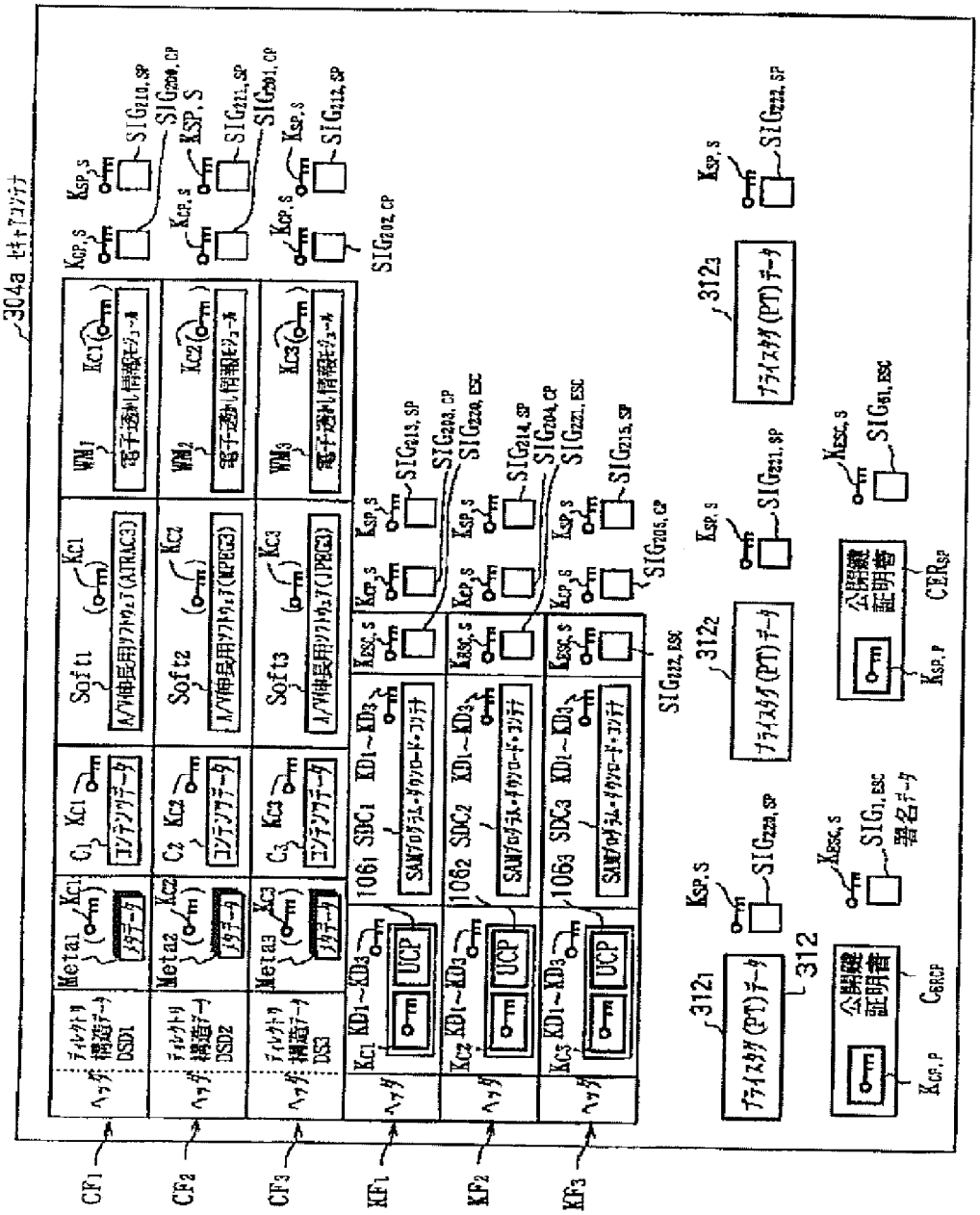
【図１１１】


104a
CF1
CF2
CF3
KF3
KF3
KF3
Meta1
Meta2
Meta3
Soft1
Soft2
Soft3
WM1
WM2
WM3
SDC1
SDC2
SDC3
UCP
公開鍵証明書
CERKCP
署名データ

【図１１３】

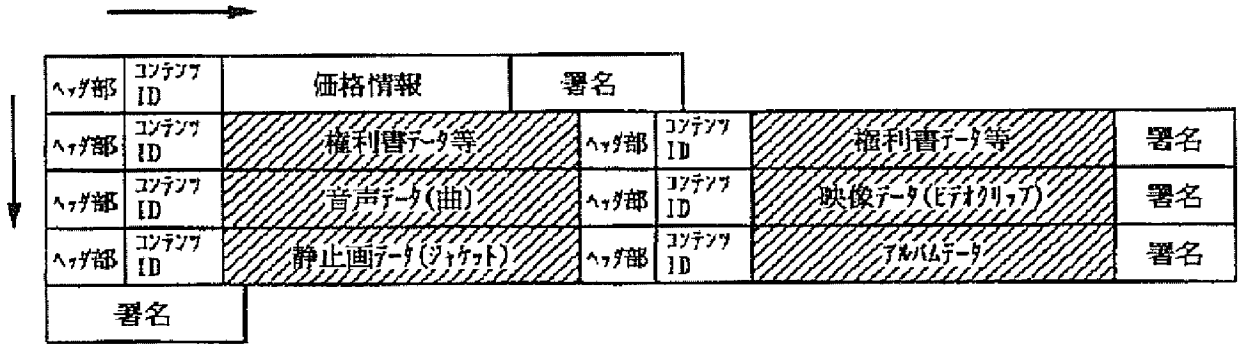

Content
暗合化
楽曲(音声) ATRAC3
Content ID
meta_data
Content
ATRAC3ﾃﾞｺｰﾀﾞ
SIG(署名ﾃﾞｰﾀ)
CF1
Secure Container Hyper Link
ビデオクリップ(映像) MPEG2
MPEG2ﾃﾞｺｰﾀﾞ
CF2
ジャケット(静止画) JPEG
JPEGﾃﾞｺｰﾀﾞ
CF3
歌詞カード(テキスト) Text(ASCII-code etc)
テキストデコーダ
CF4
商品----▶商品へのリンク
ライナーノーツ(テキスト) Text(ASCII-code etc)
CF5
配信用鍵データ
KD
SAM
KF1
Kc1
Usage Control Policy(UCP)
SAM download container
SIG
ビデオクリップ(映像)の鍵ファイル
Kc2
KF2
ジャケット(静止画)の鍵ファイル
Kc3
KF3
歌詞カードの鍵ファイル
Kc4
KF4
ライナーノーツの鍵ファイル
Kc5
KF5

【図１１４】

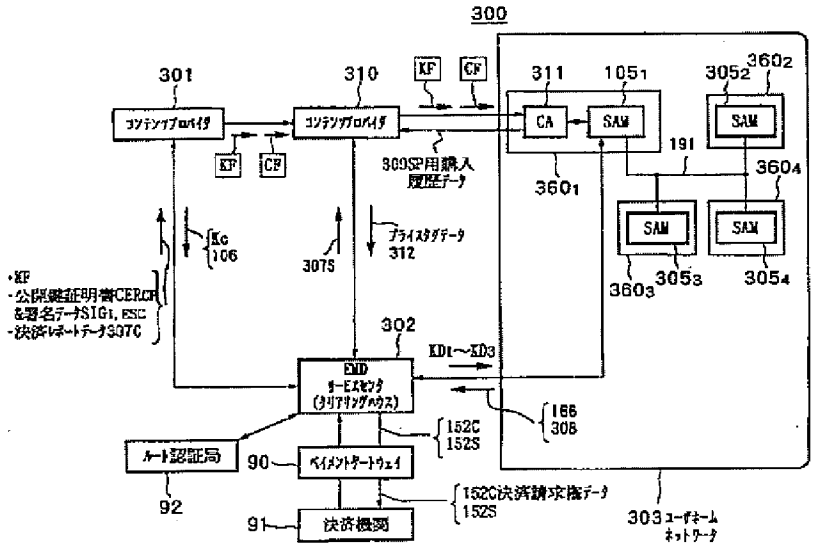


【図１１６】

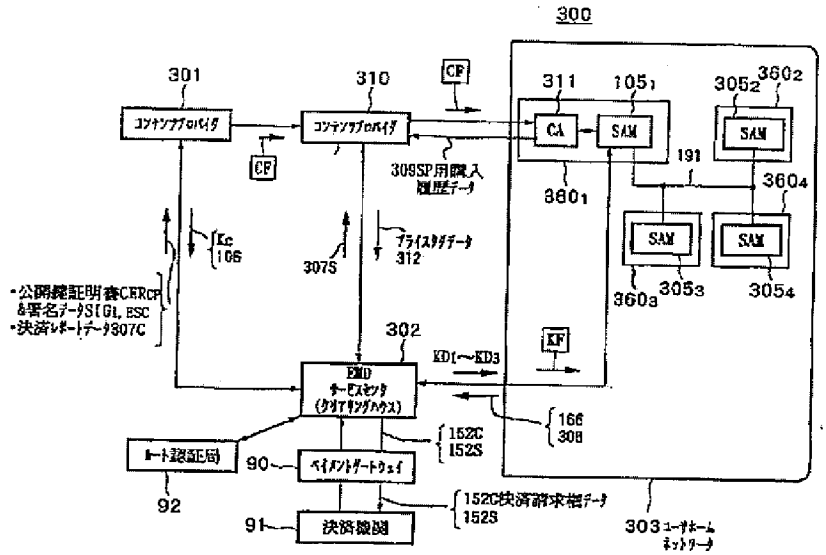
セキュアコンテナ（コンポジット型）のデータフォーマット－②



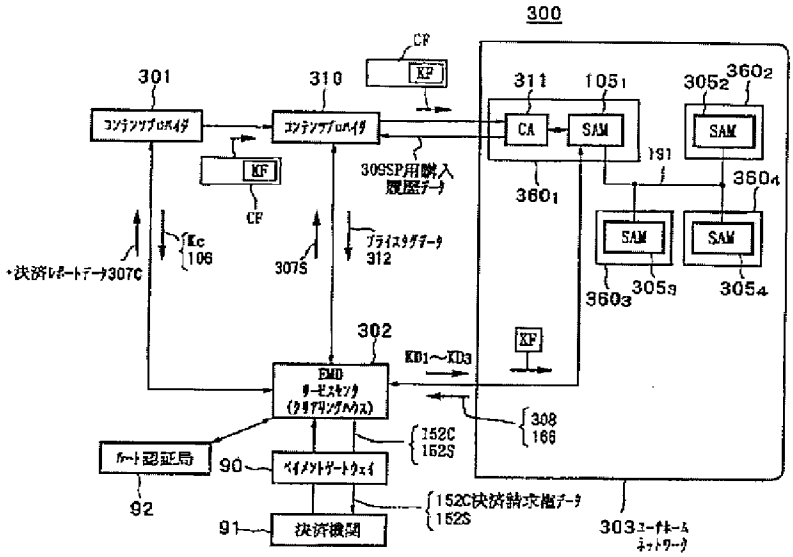
【図１１７】



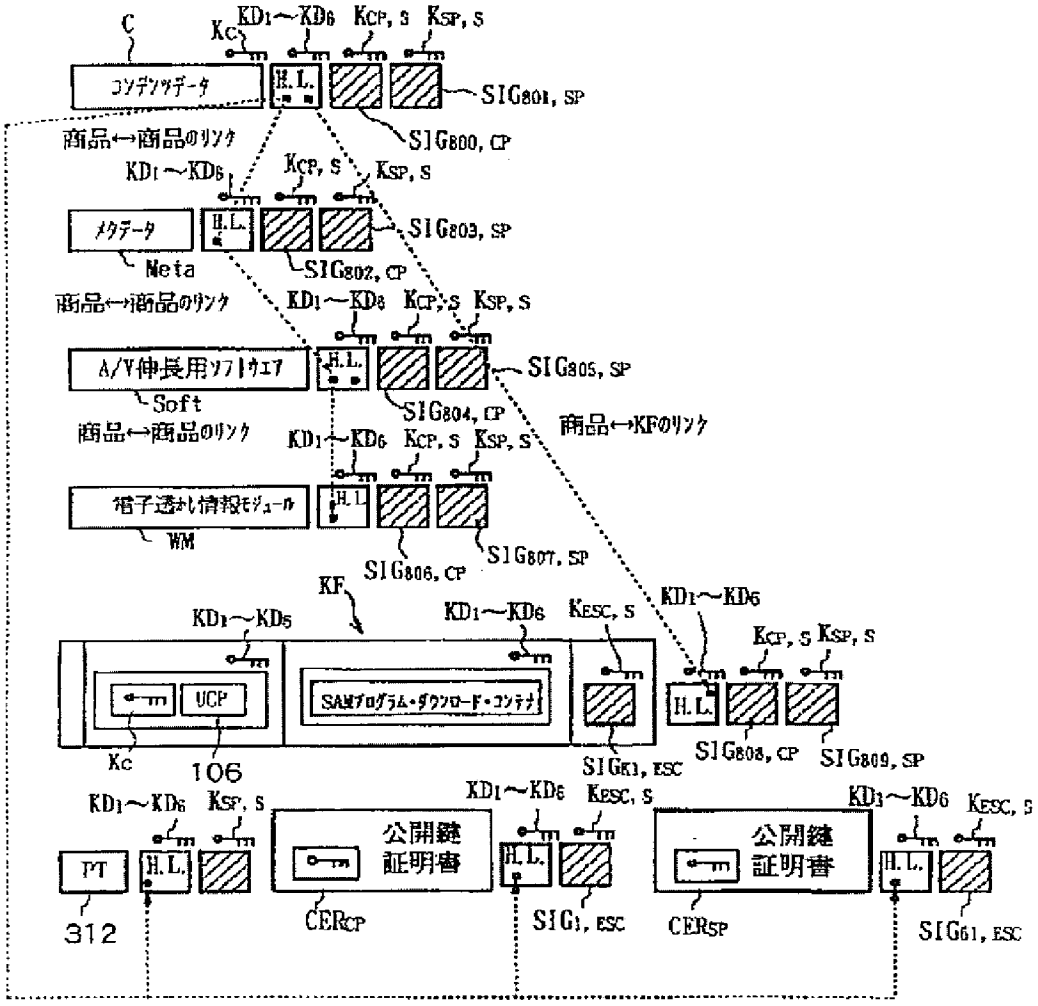
【図１１８】


300
301
310
CF
311
105₁
305₂
360₂
CA
SAM
191
360₄
309SP用購入履歴データ
360₁
Kc
106
307S
プライスタグデータ
312
SAM
SAM
SAM
360₃
305₃
305₄
・公開鍵証明書CERCP
&署名データS(G), ESC
・決済レポートデータ307C
302
KD1～KD3
KF
EMD
サービスセンタ
(クリアリングハウス)
166
308
152C
152S
ゲートウェイ
90
92
91
決済機関
152C決済請求額データ
152S
303ユーザホーム
ネットワーク

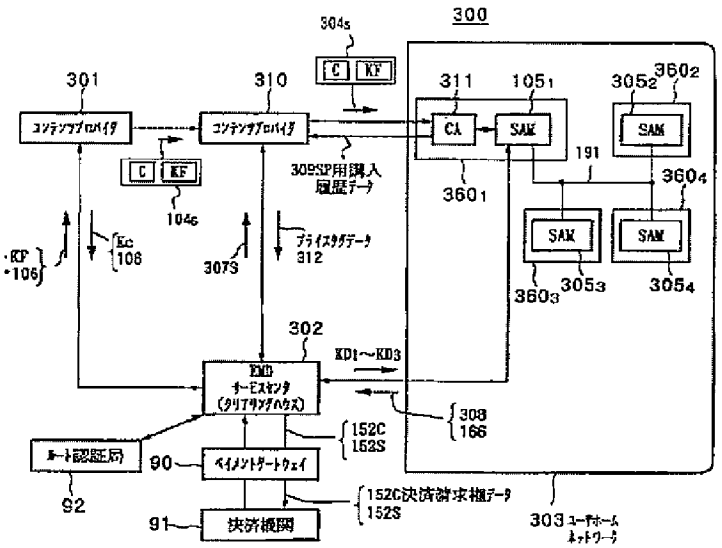
【図１２０】


300
CF
KF
301
310
311
105₁
305₂
360₂
CA
SAM
191
360₄
309SP用購入履歴データ
360₁
・決済レポートデータ307C
Kc
106
307S
プライスタグデータ
312
SAM
SAM
SAM
360₃
305₃
305₄
302
KD1～KD3
EMD
サービスセンタ
(クリアリングハウス)
308
166
152C
152S
ゲートウェイ
90
92
91
決済機関
152C決済請求額データ
152S
303ユーザホーム
ネットワーク

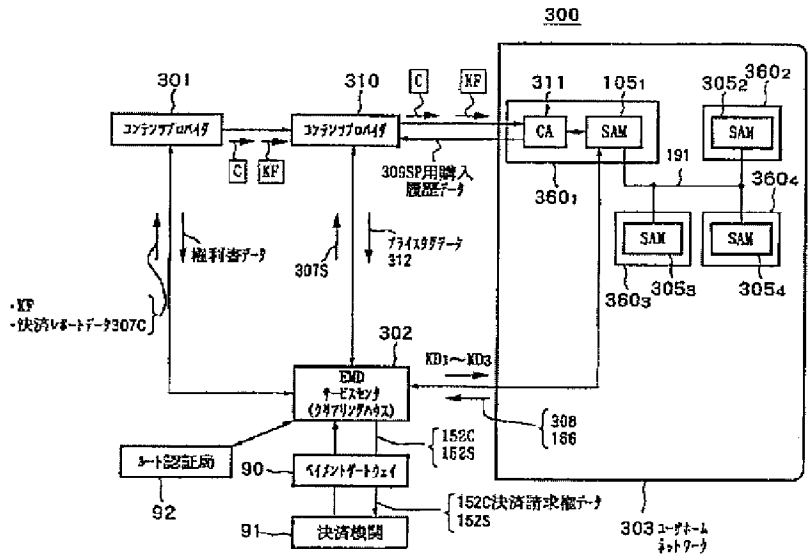
【図１１９】


C
Kc
KD1～KD6
KCP, S
KSP, S
コンテンツデータ
H.L.
SIG801, SP
SIG800, CP
商品↔商品のリンク
KD1～KD6
KCP, S
KSP, S
メタデータ
H.L.
SIG803, SP
Meta
SIG802, CP
商品↔商品のリンク
KD1～KD6
KCP, S
KSP, S
A/V伸長用ソフトウエア
H.L.
SIG805, SP
Soft
SIG804, CP
商品↔商品のリンク
KD1～KD6
KCP, S
KSP, S
商品↔KFのリンク
電子透かし情報モジュール
H.L.
WM
SIG806, CP
SIG807, SP
KF
KD1～KD5
KD1～KD6
KESC, S
KD1～KD6
KCP, S
KSP, S
UCP
SAMプログラム・ダウンロード・コンテナ
H.L.
Kc
106
SIGK1, ESC
SIG808, CP
SIG809, SP
KD1～KD6
KSP, S
KD1～KD6
KESC, S
KD1～KD6
KESC, S
PT
H.L.
公開鍵証明書
H.L.
公開鍵証明書
H.L.
312
CERCP
SIG1, ESC
CERSP
SIG61, ESC

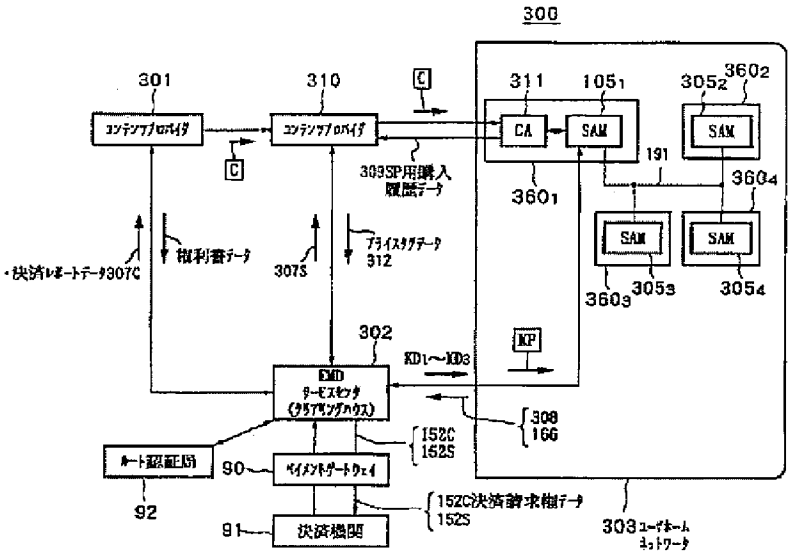
【図１２１】


300
304S
C
KF
301
310
311
105₁
305₂
360₂
CA
SAM
191
360₄
309SP用購入履歴データ
360₁
104S
Kc
108
307S
プライスタグデータ
312
KF
106
SAM
360₃
305₃
305₄
302
KD1～KD3
EMD
サービスセンタ
(クリアリングハウス)
308
166
152C
152S
ルート認証局
90
ペイメントゲートウェイ
92
152C決済請求権データ
152S
91
決済機関
303 ユーザホーム
ネットワーク

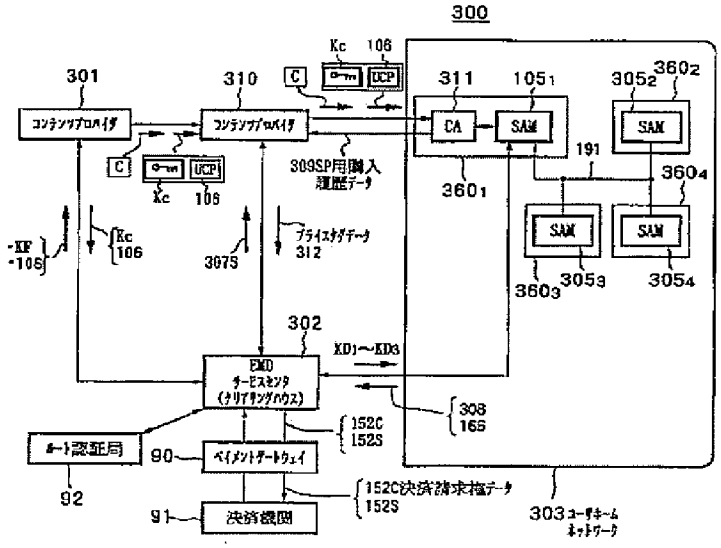
【図１２２】


300
301
310
C
KF
311
105₁
305₂
360₂
CA
SAM
191
360₄
309SP用購入履歴データ
360₁
C
KF
権利書データ
307S
プライスタグデータ
312
SAM
360₃
305₃
305₄
KF
快済レポートデータ307C
302
KD1～KD3
EMD
サービスセンタ
(クリアリングハウス)
308
166
152C
152S
ルート認証局
90
ペイメントゲートウェイ
92
152C決済請求権データ
152S
91
決済機関
303 ユーザホーム
ネットワーク

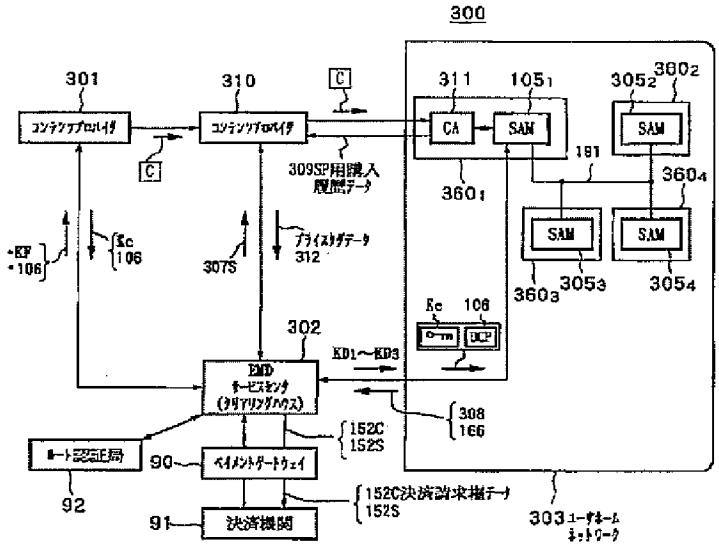
【図１２３】


300
301
310
C
311
105₁
305₂
360₂
CA
SAM
191
309SP用購入履歴データ
360₁
360₄
・決済レポートデータ307C
権利書データ
307S
プライスタグデータ312
360₃
305₃
305₄
302
KD1～KD3
KP
EMD
サービスセンタ
(クリアリングハウス)
308
166
152C
152S
ポート認証局
90
ペイメントゲートウェイ
92
152C決済請求権データ
152S
91
決済機関
303ユーザホームネットワーク

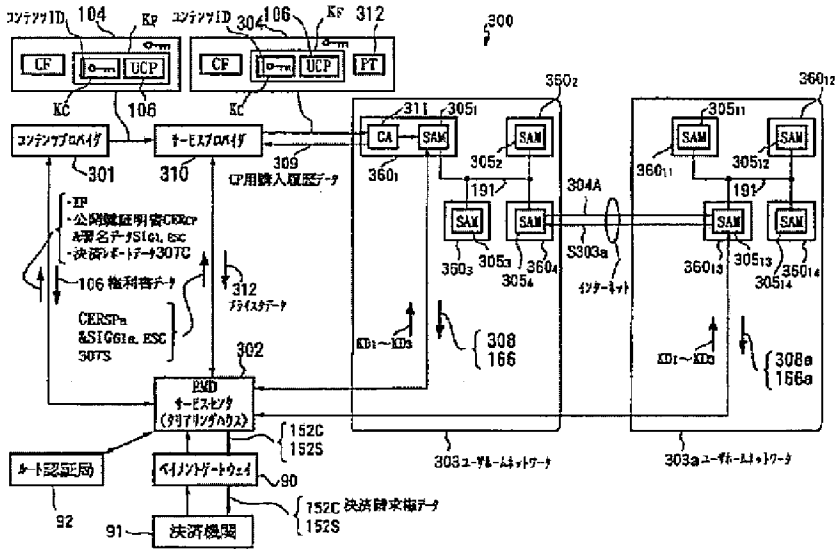
【図１２４】


300
Kc
106
301
310
C
311
105₁
305₂
360₂
CA
SAM
191
309SP用購入履歴データ
360₁
360₄
-KF
-105
Kc
106
307S
プライスタグデータ312
360₃
305₃
305₄
302
KD1～KD3
EMD
サービスセンタ
(クリアリングハウス)
308
165
152C
152S
ポート認証局
90
ペイメントゲートウェイ
92
152C決済請求権データ
152S
91
決済機関
303ユーザホームネットワーク

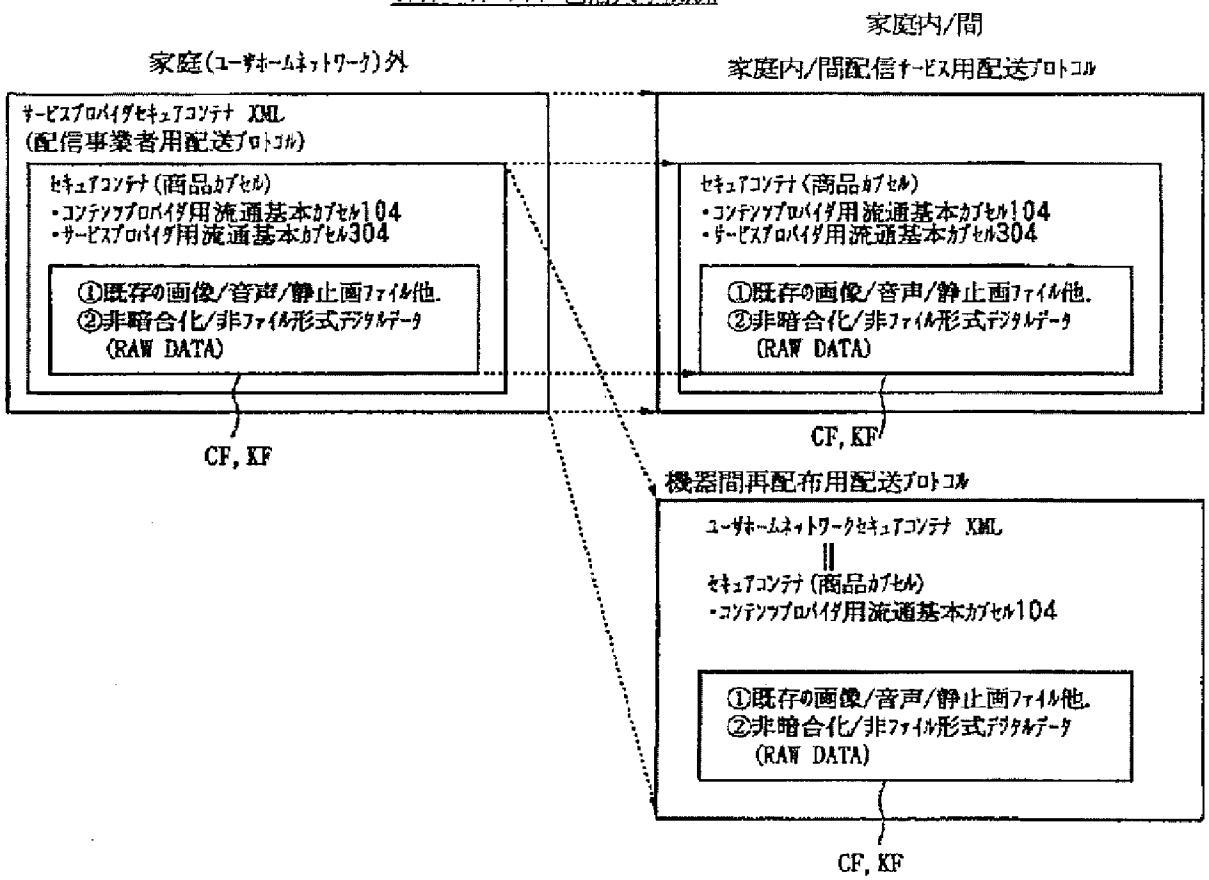
【図１２５】


300
301
310
C
311
105₁
CA
SAM
360₂
305₂
SAM
181
360₄
SAM
SAM
360₁
360₃
305₃
305₄
309SP用購入履歴データ
Kc
106
307S
プライスタグデータ
312
302
KD1～KD3
EMD
サービスセンタ
(クリアリングハウス)
308
166
152C
152S
ルート認証局
90
ペイメントゲートウェイ
92
91
決済機関
152C決済請求権データ
152S
303ユーザホームネットワーク

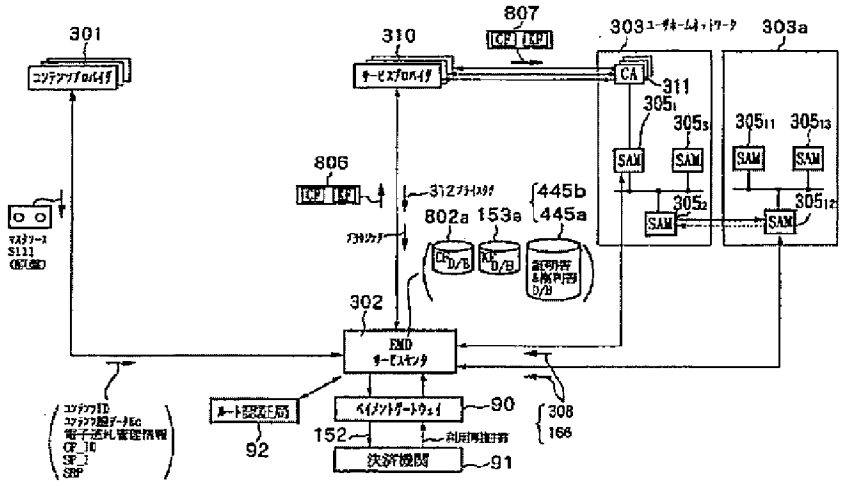
【図１２６】


コンテンツID
104
Kp
106
Ks
312
300
CF
UCP
PT
304
Kc
106
コンテンツプロバイダ
サービスプロバイダ
301
310
309
CP用購入履歴データ
360₁
311
305₁
CA
SAM
360₂
305₂
191
304A
360₁₂
305₁₁
305₁₂
360₁₁
360₃
305₃
360₄
305₄
S303a
インターネット
360₁₃
305₁₃
360₁₄
305₁₄
・IP
・公開鍵証明書CERTcp
お客名データSIGi, esc
・決済レポートデータ307C
106 権利書データ
312
プライスタグデータ
CERTSPn
&SIGGIn, ESC
307S
302
KD1～KD3
308
166
308a
166a
EMD
サービスセンタ
(クリアリングハウス)
152C
152S
ルート認証局
ペイメントゲートウェイ
90
92
91
決済機関
152C 決済請求権データ
152S
303ユーザホームネットワーク
303aユーザホームネットワーク

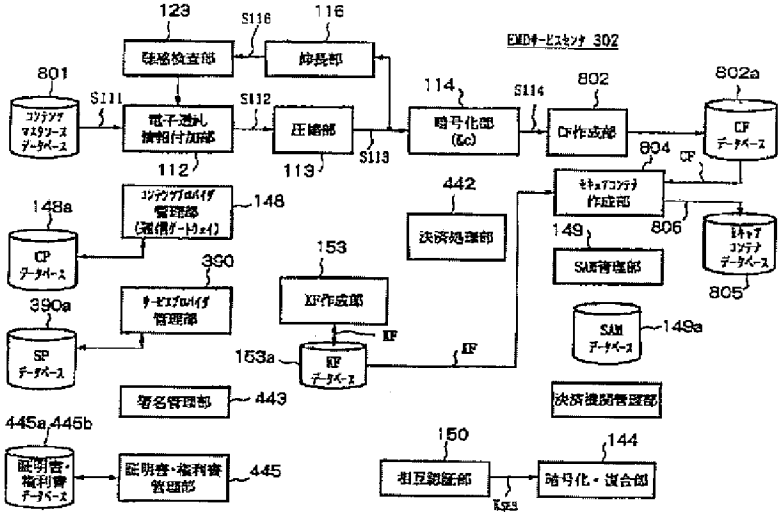
【図１２７】


セキュアコンテナのファイル包括大小関係
家庭内/間
家庭(ユーザホームネットワーク)外
家庭内/間配信サービス用配送プロトコル
サービスプロバイダセキュアコンテナ XML
(配信事業者用配送プロトコル)
セキュアコンテナ(商品カプセル)
・コンテンツプロバイダ用流通基本カプセル104
・サービスプロバイダ用流通基本カプセル304
①既存の画像/音声/静止画ファイル他.
②非暗合化/非ファイル形式デジタルデータ
(RAW DATA)
CF, KF
セキュアコンテナ(商品カプセル)
・コンテンツプロバイダ用流通基本カプセル104
・サービスプロバイダ用流通基本カプセル304
①既存の画像/音声/静止画ファイル他.
②非暗合化/非ファイル形式デジタルデータ
(RAW DATA)
CF, KF
機器間再配布用配送プロトコル
ユーザホームネットワークセキュアコンテナ XML
セキュアコンテナ(商品カプセル)
・コンテンツプロバイダ用流通基本カプセル104
①既存の画像/音声/静止画ファイル他.
②非暗合化/非ファイル形式デジタルデータ
(RAW DATA)
CF, KF

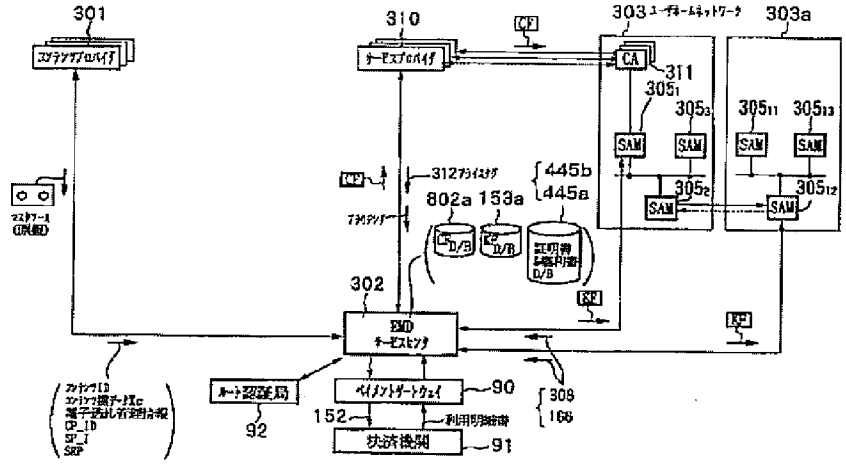
【図１２８】


301
310
807
303
303a
CA
311
SAM
806
445b
445a
153a
802a
302
90
91
92
152
308
166

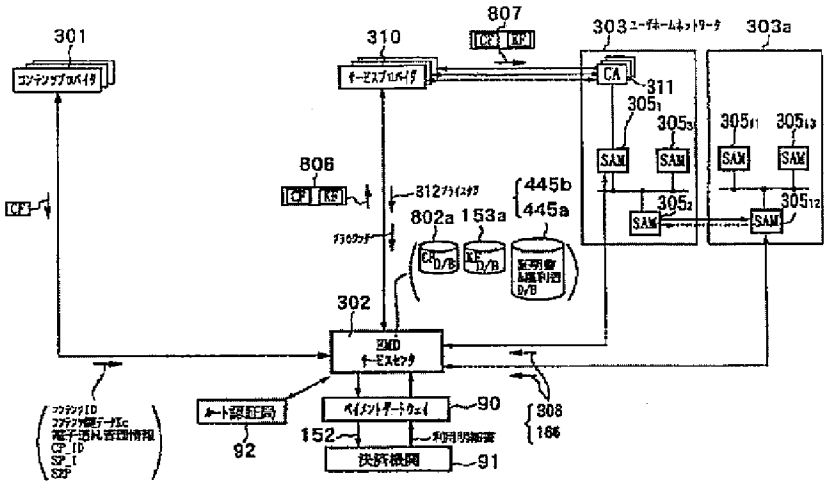
【図１２９】



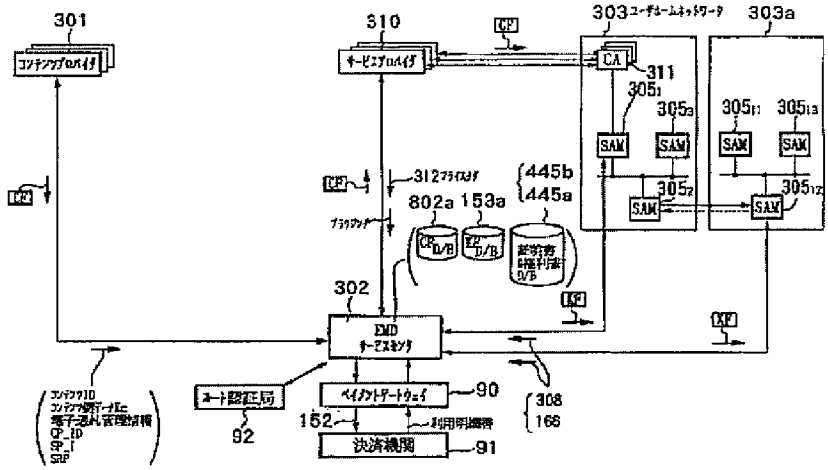
【図１３０】



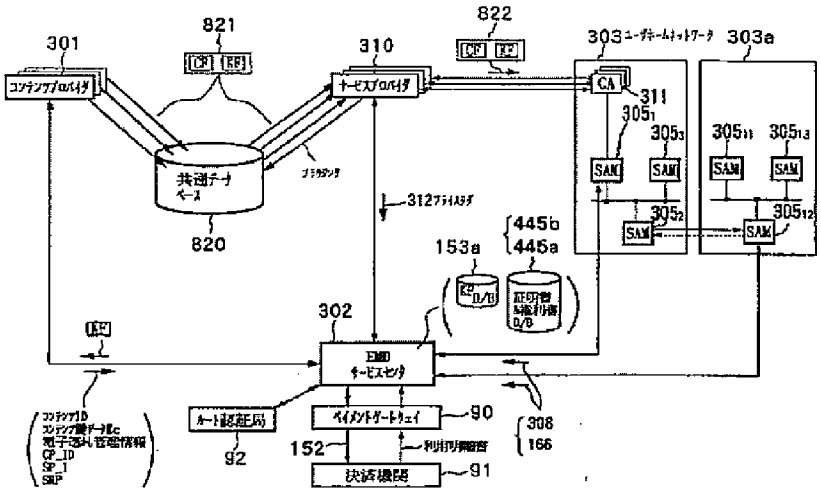
【図１３１】


301
310
807
303
303a
CA
311
806
312
445b
445a
802a
153a
302
SAM
90
91
92
152
308
166

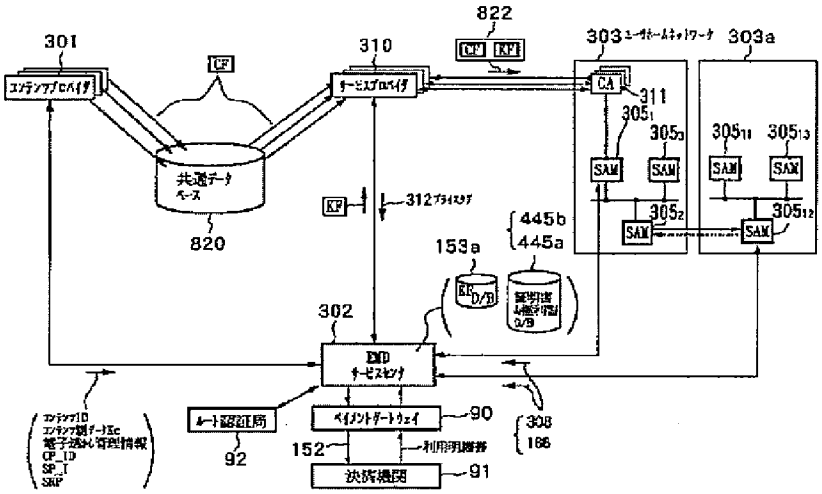
【図１３２】


301
310
303
303a
CA
311
312
445b
445a
802a
153a
302
SAM
90
91
92
152
308
166

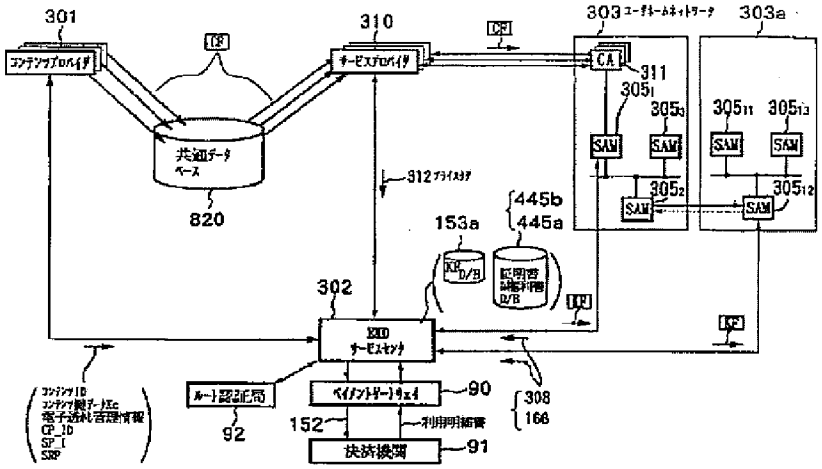
【図１３３】


301
821
822
310
303
303a
820
312
153a
445b
445a
302
90
91
92
152
308
166
CA
311
SAM

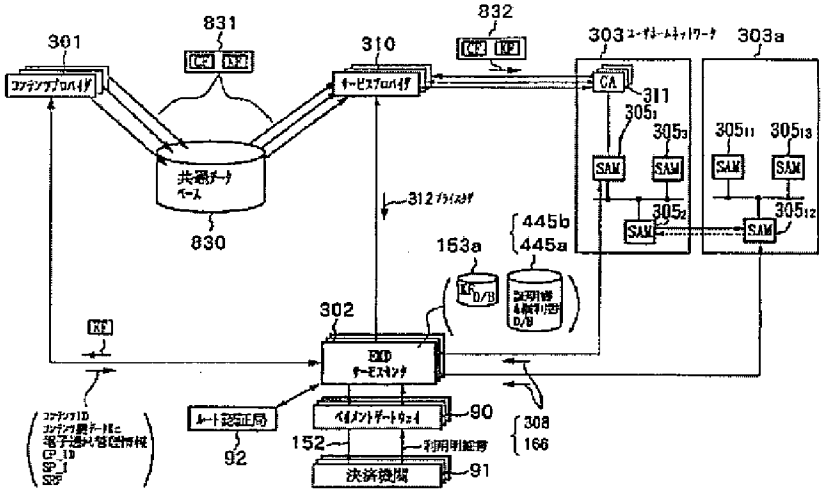
【図１３４】


301
822
310
303
303a
820
312
153a
445b
445a
302
90
91
92
152
308
166
CA
311
SAM

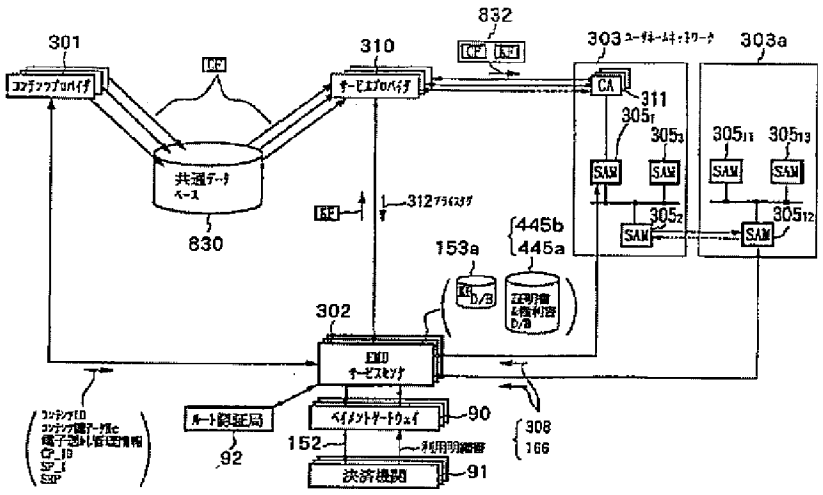
【図１３５】


301
310
303
303a
311
820
312
445b
445a
153a
302
90
92
152
91
308
166

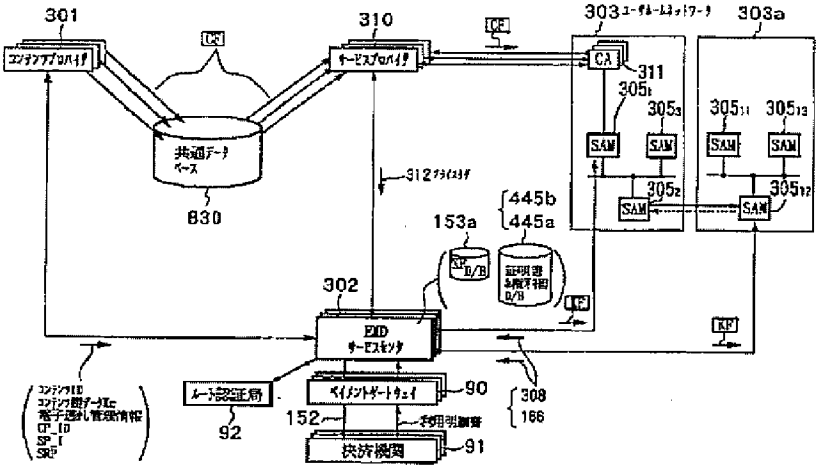
【図１３６】


831
832
301
310
303
303a
311
830
312
445b
445a
153a
302
90
92
152
91
308
166

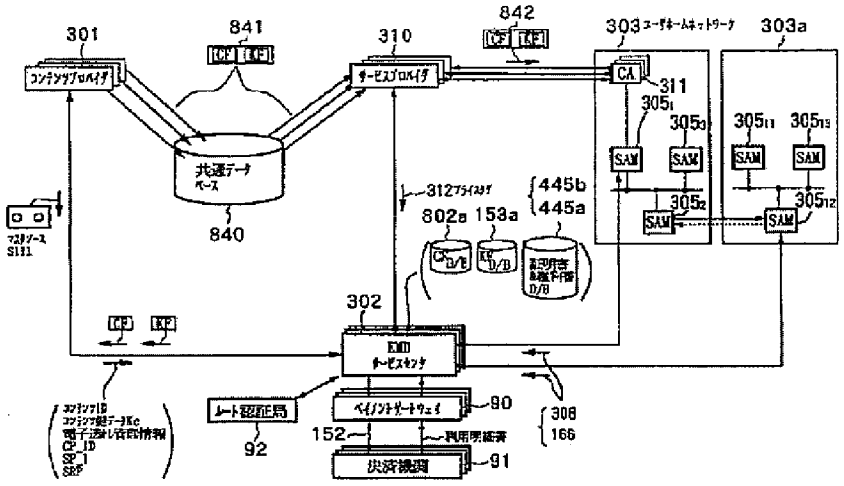
【図１３７】


832
301
310
303
303a
CA
311
SAM
630
312
153a
445b
445a
302
90
92
152
91
308
166

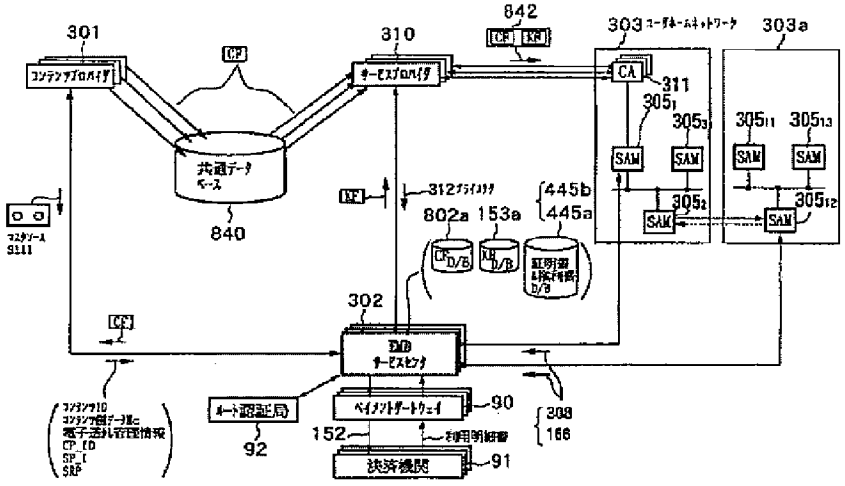
【図１３８】


301
310
303
303a
CA
311
SAM
630
312
153a
445b
445a
302
90
92
152
91
308
166

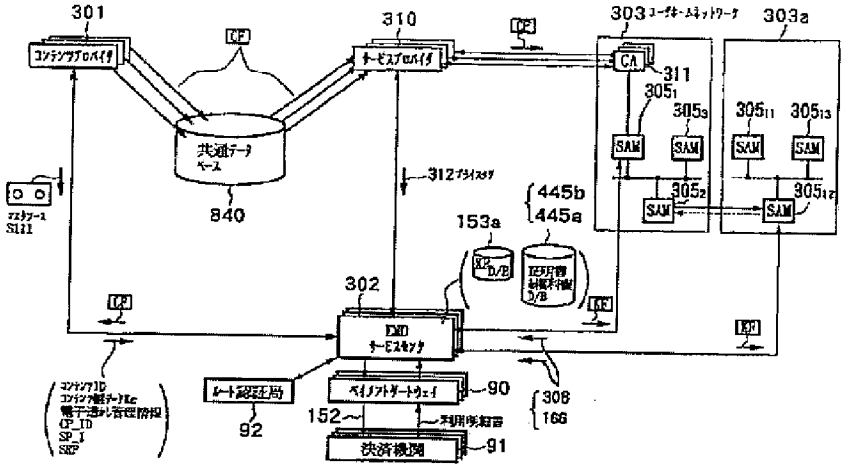
【図１３９】


301
841
310
842
303
303a
CA
311
SAM
共通データベース
840
312
445b
445a
802a
153a
302
90
92
152
91
308
166

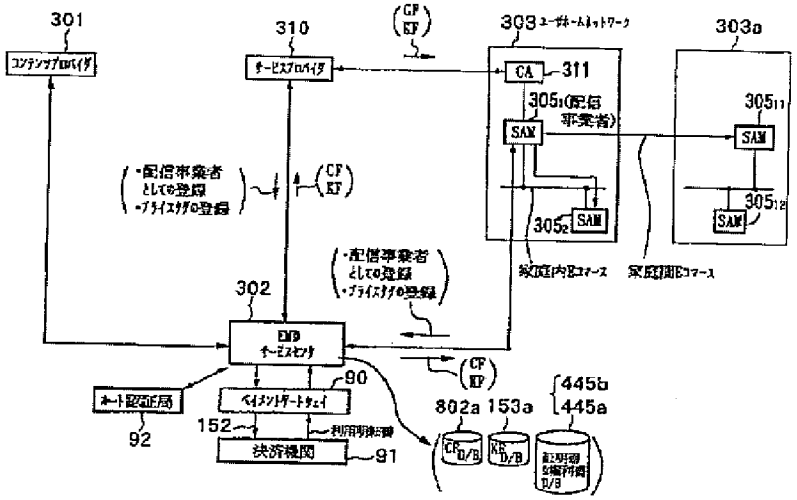
【図１４０】


301
310
842
303
303a
CA
311
SAM
共通データベース
840
312
445b
445a
802a
153a
302
90
92
152
91
308
166

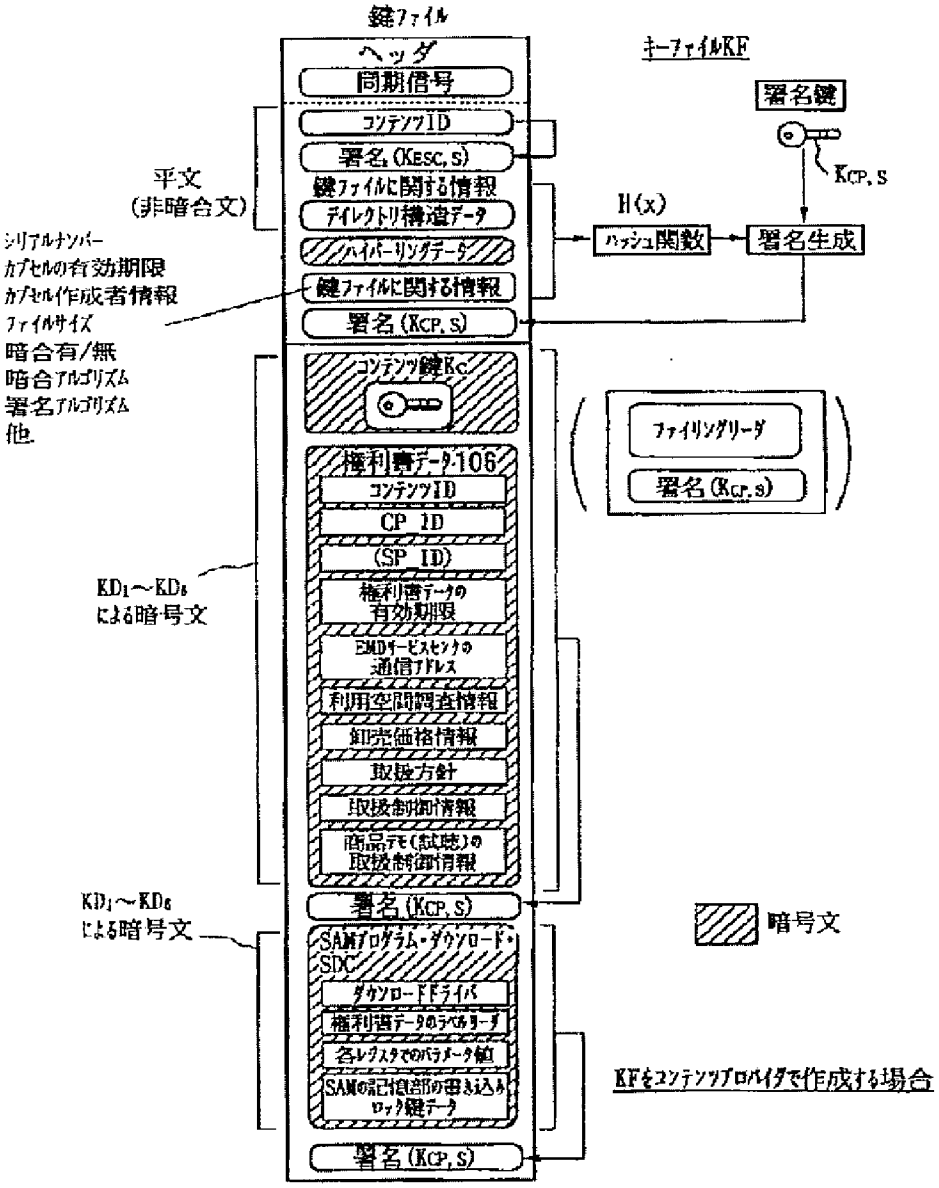
【図１４１】


301
310
303
303a
311
840
312
445b
445a
153a
302
90
92
91
152
308
166

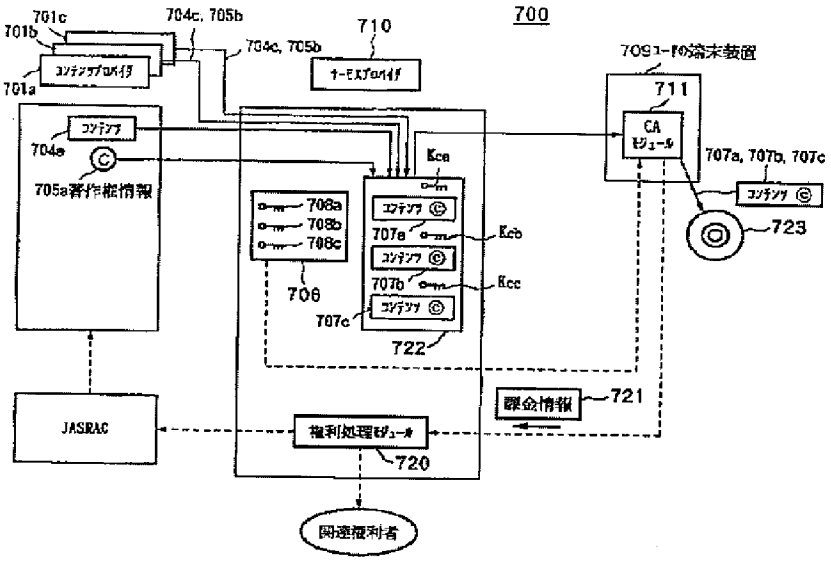
【図１４２】


301
310
303
303a
311
302
90
92
91
152
802a
153a
445b
445a

【図１４４】

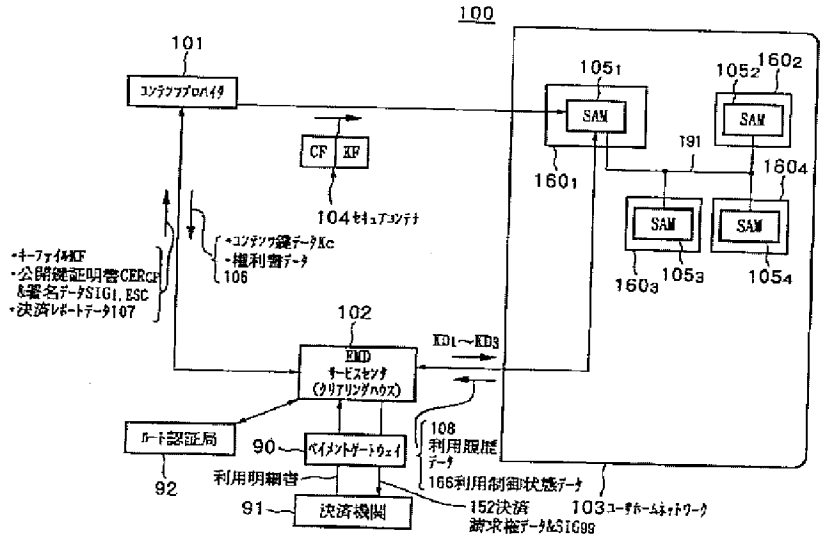

鍵ファイル
ヘッダ
同期信号
コンテンツID
署名1 (KESC, S)
鍵ファイルに関する情報
ディレクトリ構造データ
ハイパーリンクデータ
鍵ファイルに関する情報
署名 (KCP, S)
平文
(非暗合文)
シリアルナンバー
カプセルの有効期限
カプセル作成者情報
ファイルサイズ
暗合有/無
暗合アルゴリズム
署名アルゴリズム
他
コンテンツ鍵Kc
権利書データ106
コンテンツID
CP ID
(SP ID)
権利書データの有効期限
EMDサービスセンタの通信アドレス
利用空間調査情報
卸売価格情報
取扱方針
取扱制御情報
商品デモ(試聴)の取扱制御情報
署名 (KCP, S)
SAM用プログラム・ダウンロード・SDC
ダウンロードドライバ
権利書データのラベルヨーダ
各レジスタでのパラメータ値
SAMの記憶部の書き込みロック鍵データ
署名 (KCP, S)
KD1～KD8による暗号文
KD1～KD8による暗号文
キーファイルKF
署名鍵
KCP, S
H(x)
ハッシュ関数
署名生成
ファイリングリーダ
署名 (KCP, S)
暗号文
KFをコンテンツプロバイダで作成する場合

【図１４５】



【手続補正書】
【提出日】平成１２年２月２８日（２０００．２．２８）
【手続補正１】
【補正対象書類名】図面
【補正対象項目名】全図
【補正方法】変更
【補正内容】

【図１】

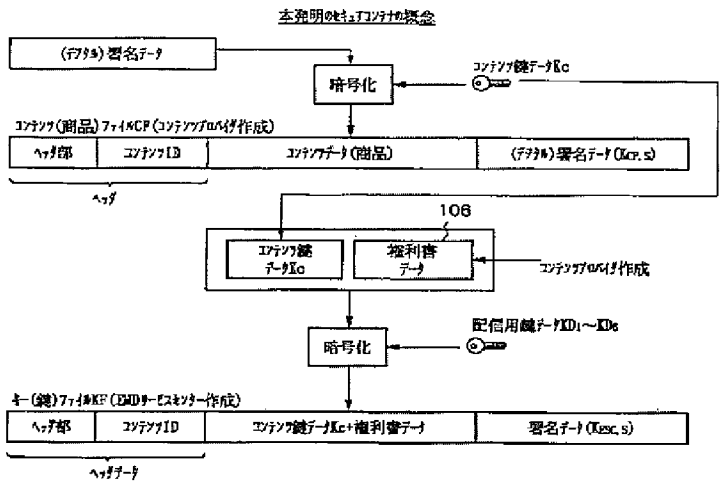


【図２７】

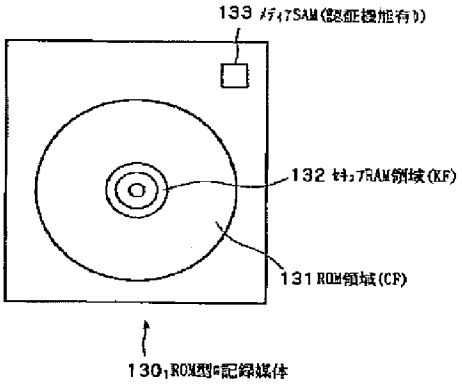
外部メモリ201に記憶されるデータ

利用履歴データ108
SAM登録リスト

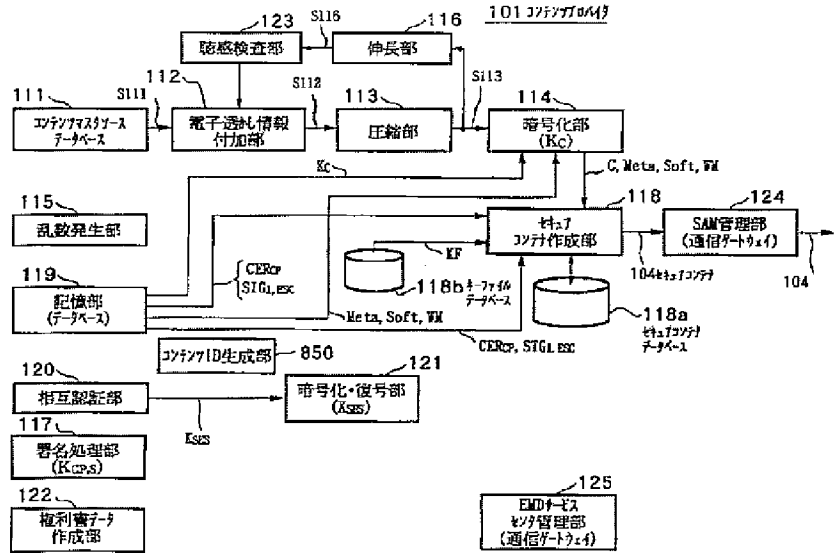
【図２】


本発明のセキュアコンテナの概念
(デジタル)署名データ
暗号化
コンテンツ鍵データKc
コンテンツ(商品)ファイルCF(コンテンツプロバイダ作成)
ヘッダ部
コンテンツID
コンテンツデータ(商品)
(デジタル)署名データ(Kcp,s)
ヘッダ
106
コンテンツ鍵データKc
権利書データ
コンテンツプロバイダ作成
暗号化
配信用鍵データKD1～KDn
キー(鍵)ファイルKF(EMDサービスセンター作成)
ヘッダ部
コンテンツID
コンテンツ鍵データKc+権利書データ
署名データ(Ksc,s)
ヘッダデータ

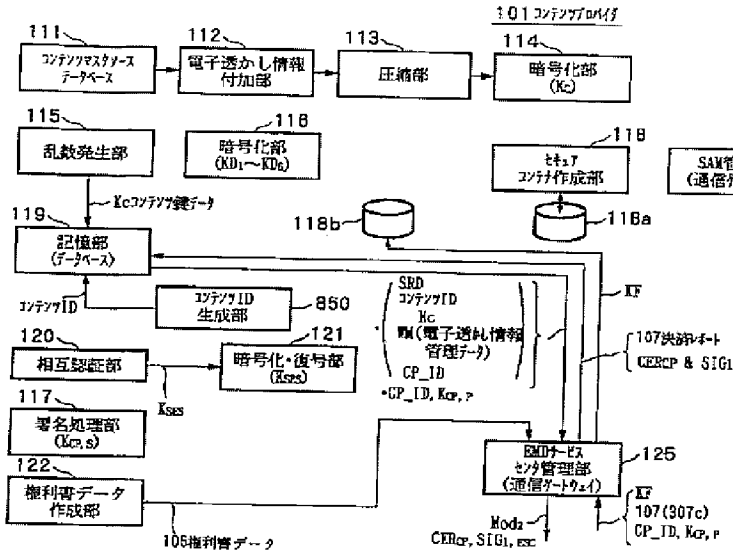
【図１２】


133 メディアSAM(認証機能有り)
132 セキュアRAM領域(KF)
131 ROM領域(CF)
130 ROM型の記録媒体

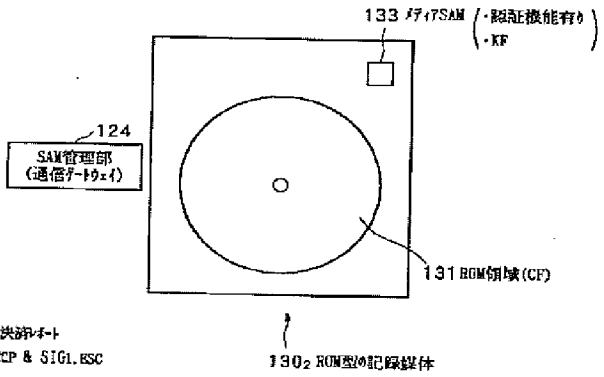
【図３】


101 コンテンツプロバイダ
123
S116
116
暗号検査部
伸長部
S113
112
S111
S112
113
114
111
コンテンツマスタソース データベース
電子透かし情報付加部
圧縮部
暗号化部 (Kc)
Kc
C, Meta, Soft, WM
115
乱数発生部
118
124
セキュアコンテナ作成部
SAM管理部 (通信ゲートウェイ)
KF
CERCP STGL,ESC
118b キーファイルデータベース
104 セキュアコンテナ
104
119
記憶部 (データベース)
Meta, Soft, WM
CERCP, STGL,ESC
118a セキュアコンテナデータベース
コンテンツID生成部
850
120
121
相互認証部
暗号化・復号部 (Kses)
Kses
117
署名処理部 (Kcp,s)
122
権利書データ作成部
125
EMDサービスセンタ管理部 (通信ゲートウェイ)

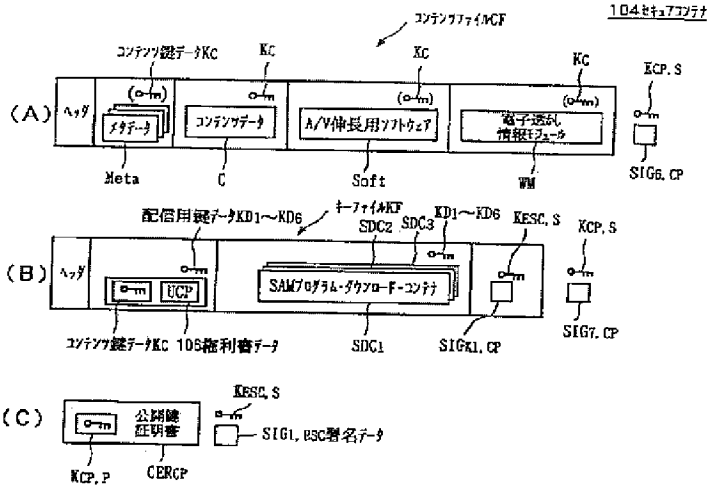
【図４】



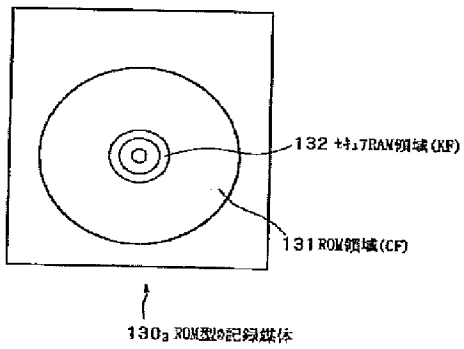
【図１３】



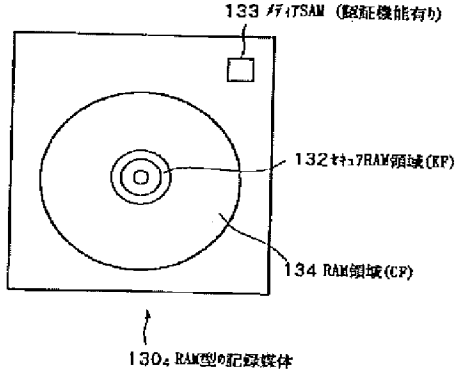
【図５】



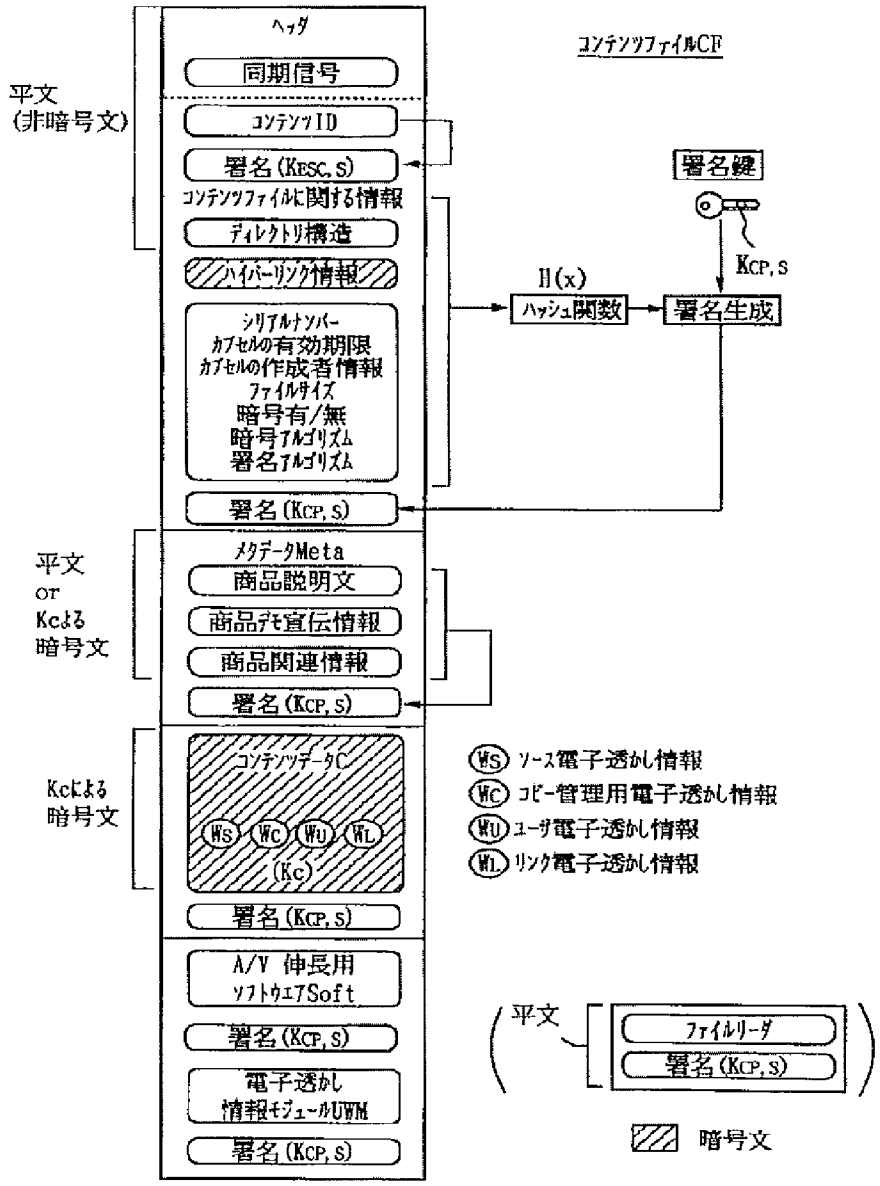
【図１４】



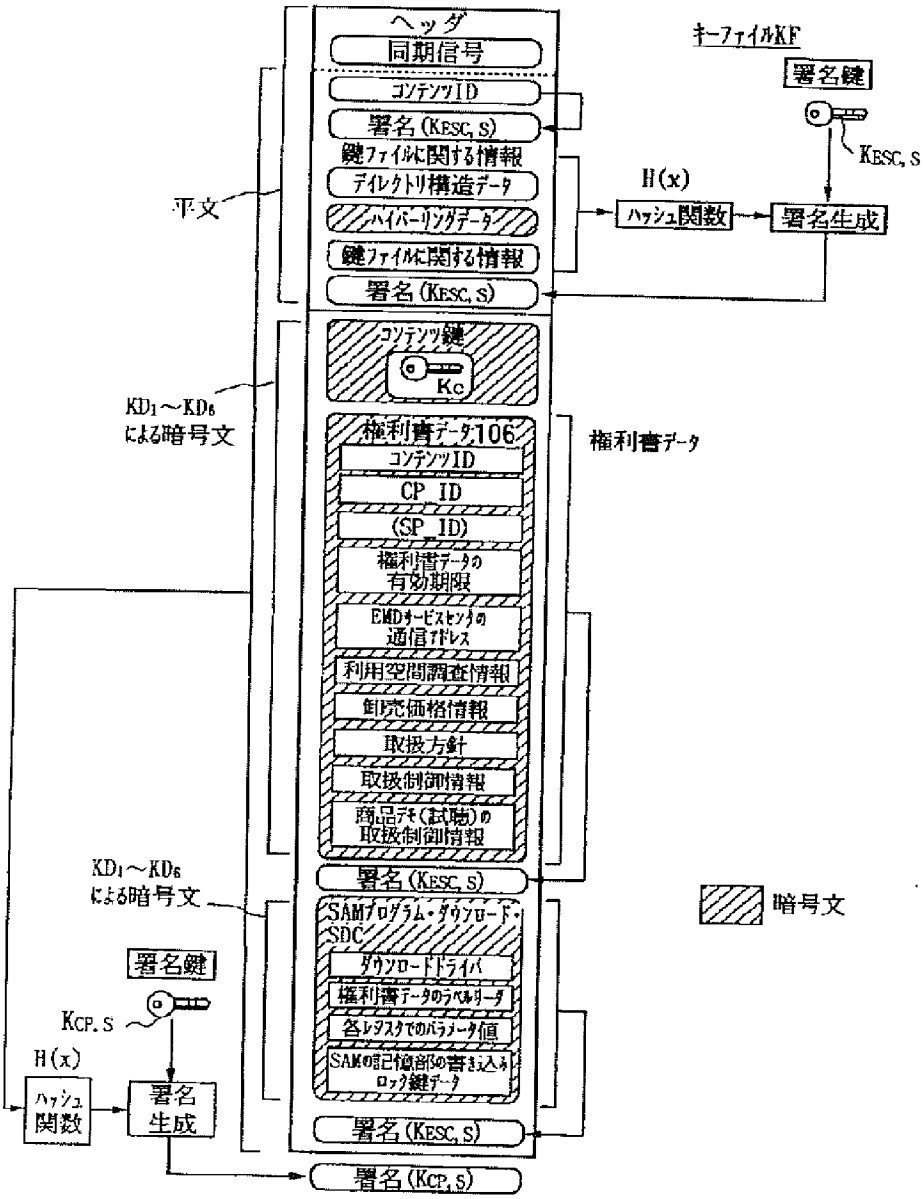
【図１５】



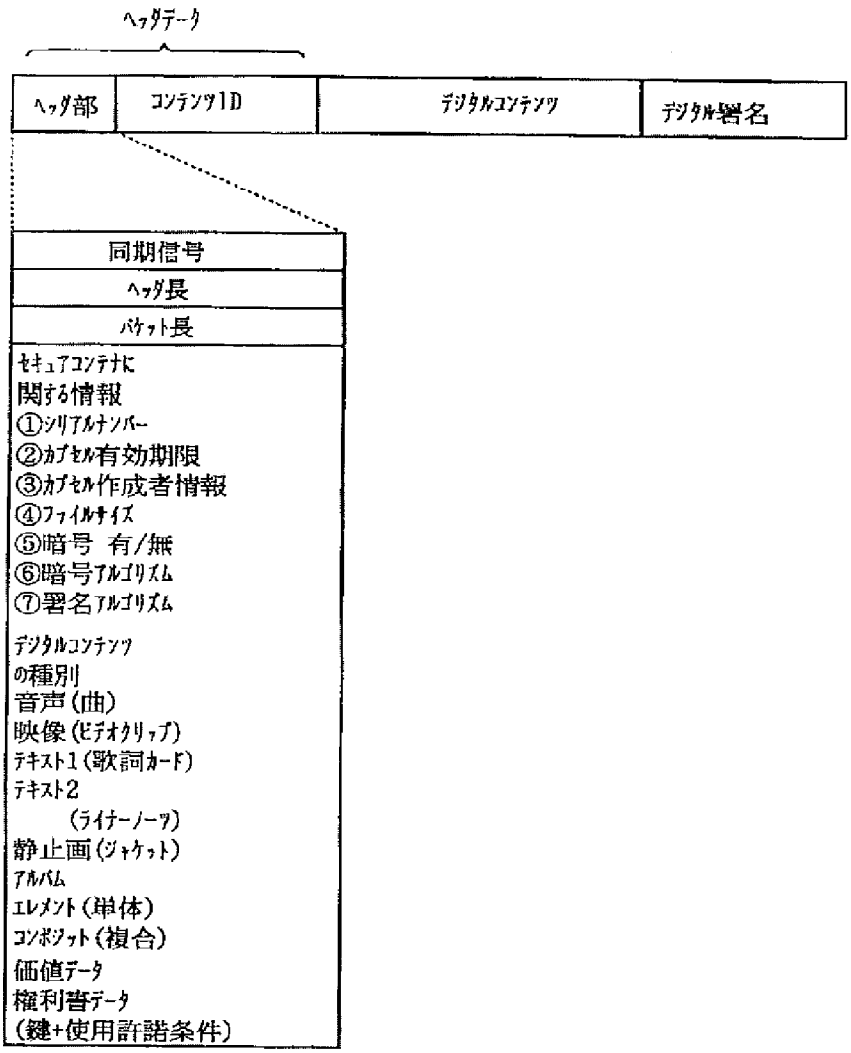
【図６】


ヘッダ
コンテンツファイルCF
同期信号
平文
(非暗号文)
コンテンツID
署名(KESC, S)
コンテンツファイルに関する情報
ディレクトリ構造
ハイパーリンク情報
シリアルナンバー
カプセルの有効期限
カプセルの作成者情報
ファイルサイズ
暗号有/無
暗号アルゴリズム
署名アルゴリズム
署名鍵
KCP, S
H(x)
ハッシュ関数
署名生成
署名(KCP, S)
メタデータMeta
平文
or
Kcよる
暗号文
商品説明文
商品デモ宣伝情報
商品関連情報
署名(KCP, S)
コンテンツデータC
Kcによる
暗号文
WS WC WU WL
(Kc)
署名(KCP, S)
WS ソース電子透かし情報
WC コピー管理用電子透かし情報
WU ユーザ電子透かし情報
WL リンク電子透かし情報
A/V 伸長用
ソフトウエアSoft
署名(KCP, S)
電子透かし
情報モジュールUWM
署名(KCP, S)
平文
ファイルリーダ
署名(KCP, S)
暗号文

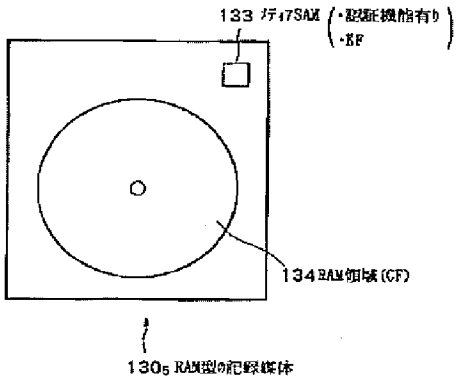
【図７】


ヘッダ
同期信号
コンテンツID
署名（KESC, S）
鍵ファイルに関する情報
ディレクトリ構造データ
ハイパーリンクデータ
鍵ファイルに関する情報
署名（KESC, S）
コンテンツ鍵
Kc
権利書データ106
コンテンツID
CP_ID
（SP_ID）
権利書データの有効期限
EMDサービスセンタの通信アドレス
利用空間調査情報
卸売価格情報
取扱方針
取扱制御情報
商品データ（試聴）の取扱制御情報
署名（KESC, S）
SAMプログラム・ダウンロード・SDC
ダウンロードドライバ
権利書データのラベルリーダ
各レジスタでのパラメータ値
SAMの記憶部の書き込みロック鍵データ
署名（KESC, S）
署名（KCP, S）
平文
KD1～KD6による暗号文
KD1～KD6による暗号文
署名鍵
KCP, S
H(x)
ハッシュ関数
署名生成
H(x)
ハッシュ関数
署名生成
キーファイルKF
署名鍵
KESC, S
権利書データ
暗号文

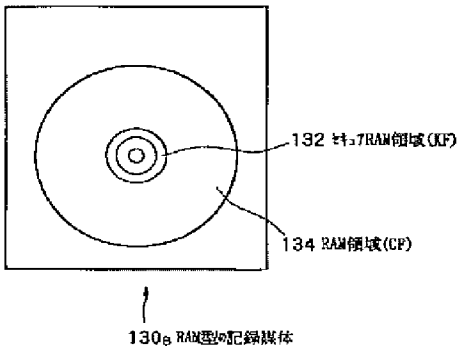
【図８】


ヘッダデータ
ヘッダ部
コンテンツID
デジタルコンテンツ
デジタル署名
同期信号
ヘッダ長
パケット長
セキュアコンテナに
関する情報
①シリアルナンバー
②カプセル有効期限
③カプセル作成者情報
④ファイルサイズ
⑤暗号 有/無
⑥暗号アルゴリズム
⑦署名アルゴリズム
デジタルコンテンツ
の種別
音声(曲)
映像(ビデオクリップ)
テキスト1(歌詞カード)
テキスト2
(ライナーノーツ)
静止画(ジャケット)
アルバム
エレメント(単体)
コンポジット(複合)
価値データ
権利書データ
(鍵+使用許諾条件)

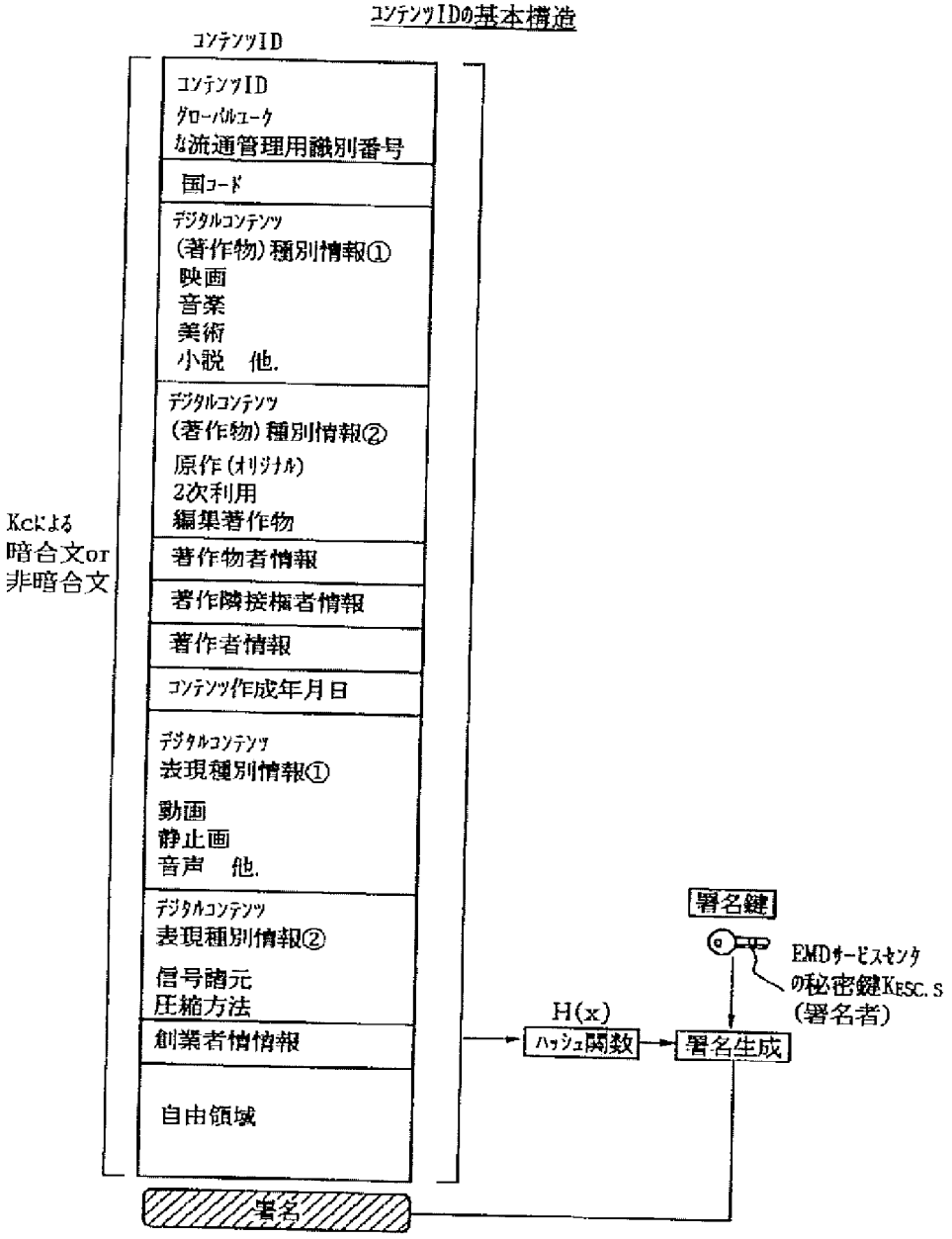
【図１６】


133 メディアSAM (・認証機能有り ・EF)
134 RAM領域(CF)
130₅ RAM型の記録媒体

【図１７】

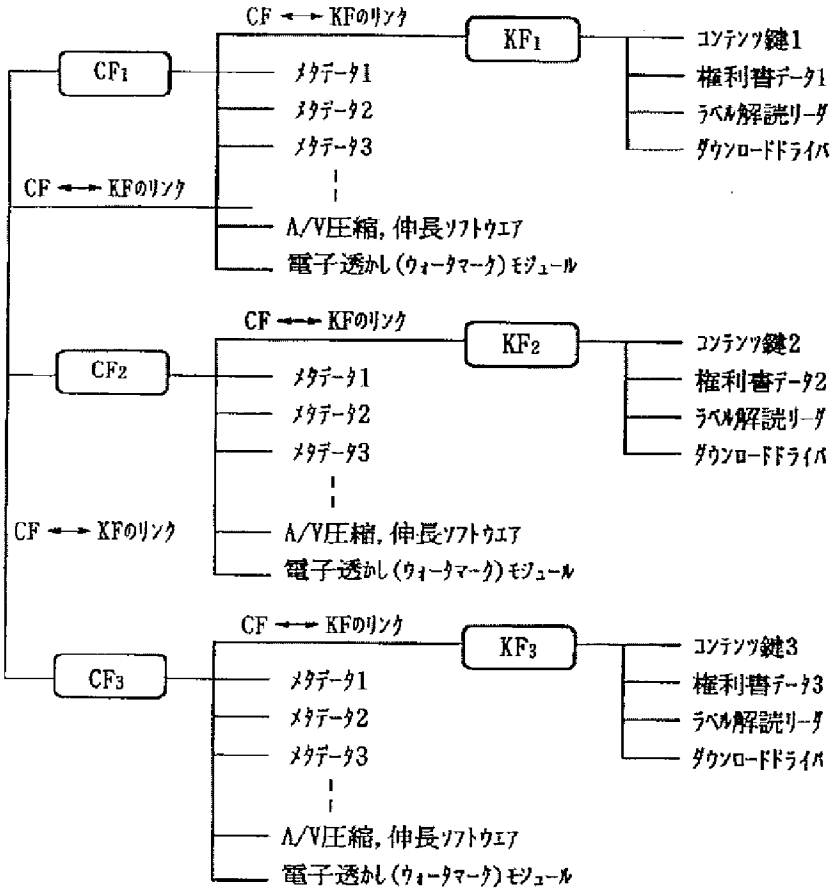

132 セキュアRAM領域(EF)
134 RAM領域(CF)
130₆ RAM型の記録媒体

【図９】


コンテンツIDの基本構造
コンテンツID
コンテンツID
グローバルユーク
な流通管理用識別番号
国コード
デジタルコンテンツ
(著作物)種別情報①
映画
音楽
美術
小説　他.
デジタルコンテンツ
(著作物)種別情報②
原作(オリジナル)
2次利用
編集著作物
著作物者情報
著作隣接権者情報
著作者情報
コンテンツ作成年月日
デジタルコンテンツ
表現種別情報①
動画
静止画
音声　他.
デジタルコンテンツ
表現種別情報②
信号諸元
圧縮方法
創業者情報情報
自由領域
署名
Kcによる
暗合文or
非暗合文
H(x)
ハッシュ関数
署名生成
署名鍵
EMDサービスセンタ
の秘密鍵KESC.S
(署名者)

【図１０】

セキュアコンテナのディレクトリ構造



【図２８】

スタックメモリ200に記憶されるデータ

コンテンツ鍵データK_C

権利書データ（UCP）106

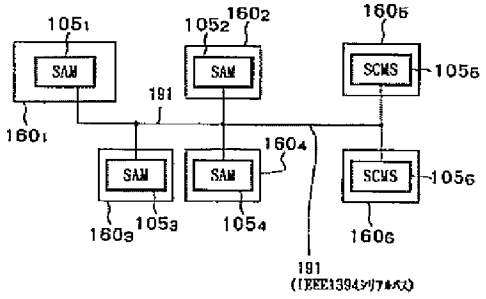
記憶部（フラッシュメモリ）192のロック鍵データK_{LOC}

コンテンツプロバイダ101の公開鍵証明書CER_{CP}

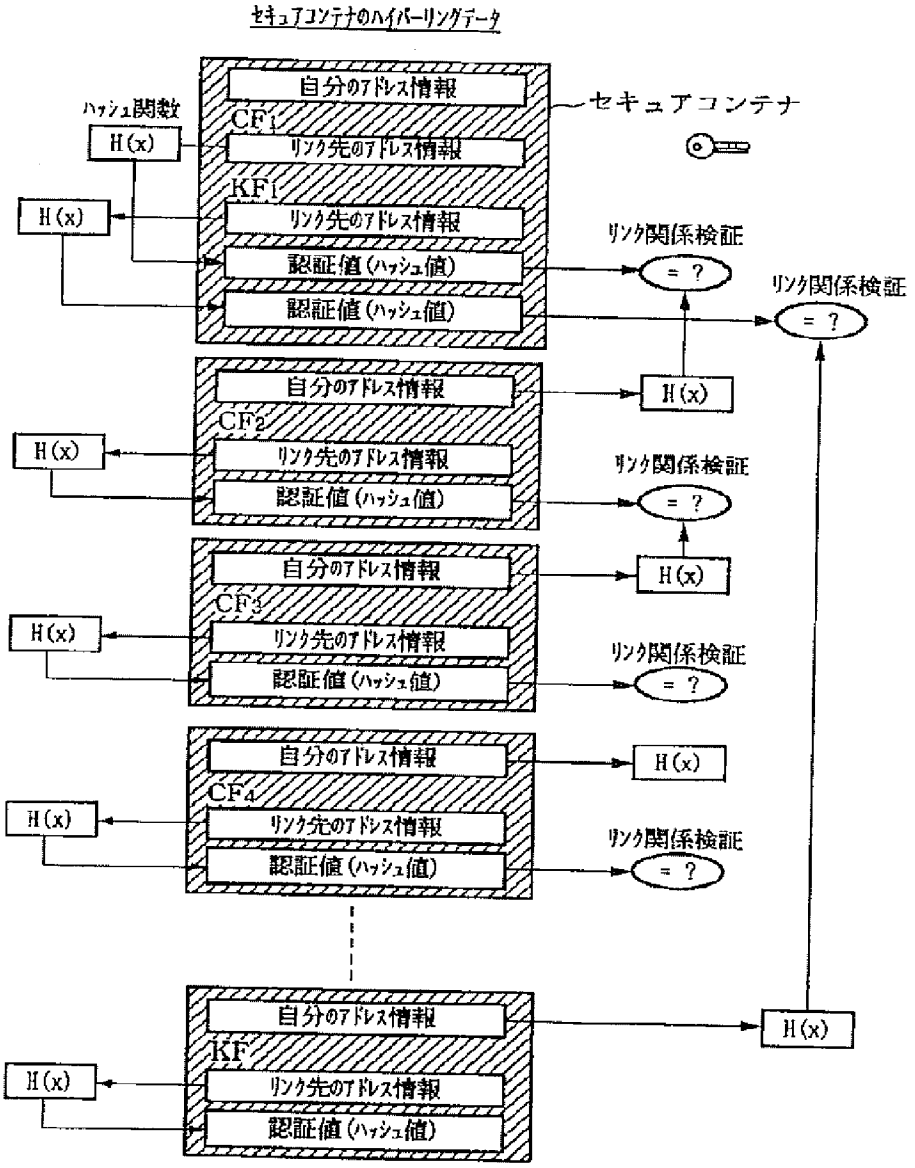
利用制御情状態データ（UCS）166

SAMプログラム・ダウンロード・コンテナSD_1～SDC_3

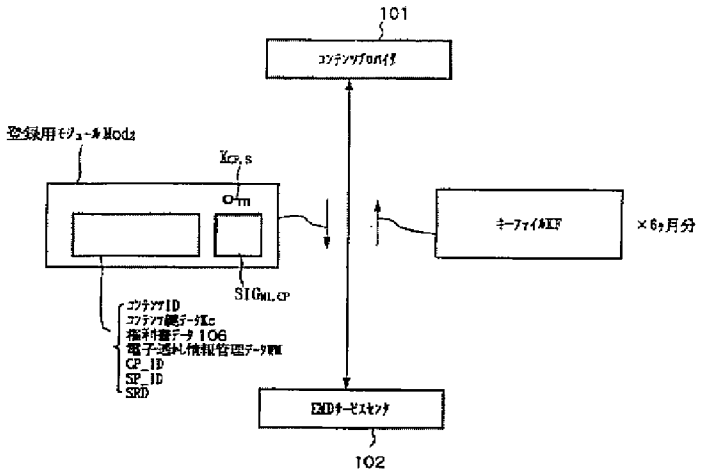
【図４４】



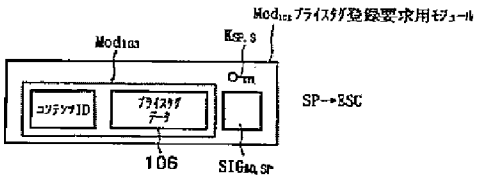
【図１１】


セキュアコンテナのハイパーリングデータ
自分のアドレス情報
ハッシュ関数
H(x)
CF1
リンク先のアドレス情報
セキュアコンテナ
KF1
リンク先のアドレス情報
認証値（ハッシュ値）
認証値（ハッシュ値）
リンク関係検証
= ?
リンク関係検証
= ?
自分のアドレス情報
H(x)
CF2
H(x)
リンク先のアドレス情報
認証値（ハッシュ値）
リンク関係検証
= ?
自分のアドレス情報
H(x)
CF3
H(x)
リンク先のアドレス情報
認証値（ハッシュ値）
リンク関係検証
= ?
自分のアドレス情報
H(x)
CF4
H(x)
リンク先のアドレス情報
認証値（ハッシュ値）
リンク関係検証
= ?
自分のアドレス情報
H(x)
KF
H(x)
リンク先のアドレス情報
認証値（ハッシュ値）

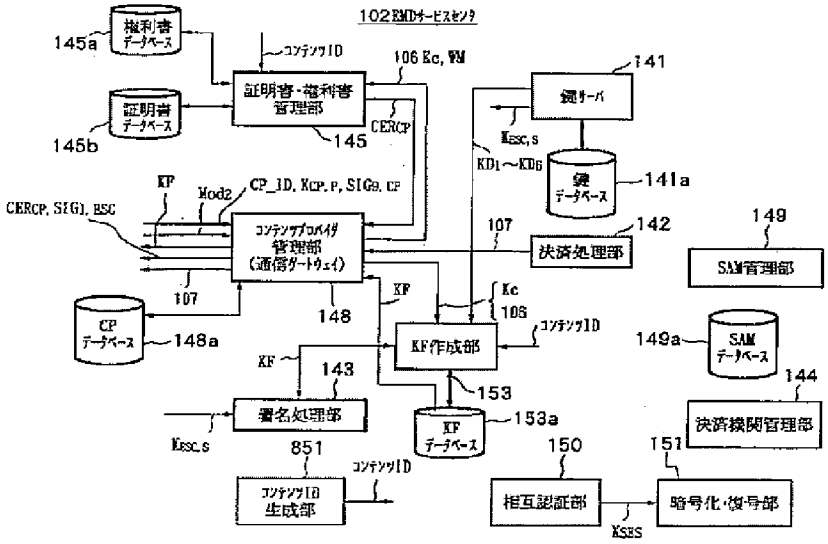
【図１８】


101
コンテンツプロバイダ
登録用モジュールMod2
Kcp, s
Otm
SIGML, CP
キーファイルKF
×6ヶ月分
コンテンツID
コンテンツ鍵データKc
権利書データ106
電子透かし情報管理データWM
CP_ID
SP_ID
SRD
EMDサービスセンタ
102

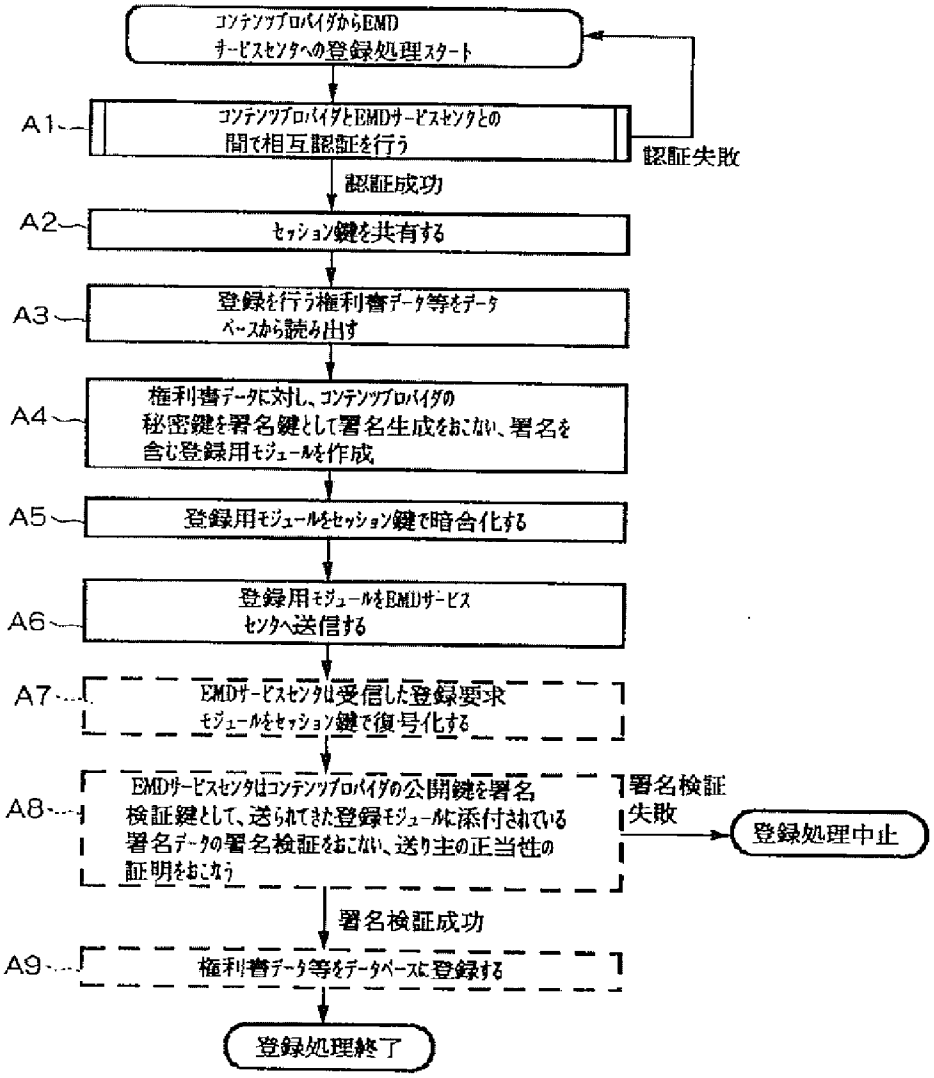
【図６９】


Mod103
Kcp, s
Otm
コンテンツID
プライスタグデータ
SP→ESC
106
SIG103, SP

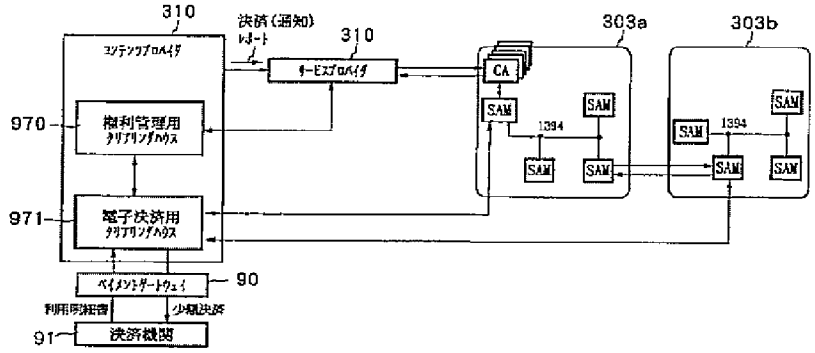
【図２３】


102 EMDサービスセンタ
145a
権利書データベース
コンテンツID
106 Kc, WM
証明書・権利書管理部
145
CERCP
145b
証明書データベース
141
鍵サーバ
Kesc, s
KD1～KD6
鍵データベース
141a
KF
Mod2
CP_ID, Kcp, p, SIG0, CP
CERCP, SIG1, ESC
コンテンツプロバイダ管理部（通信ゲートウェイ）
107
142
決済処理部
149
SAM管理部
107
148
KF
Kc
106
CP データベース
148a
KF作成部
コンテンツID
149a
SAM データベース
KF
143
153
144
署名処理部
KF データベース
153a
決済機関管理部
Kesc, s
851
150
151
コンテンツID 生成部
コンテンツID
相互認証部
暗号化・復号部
KSES

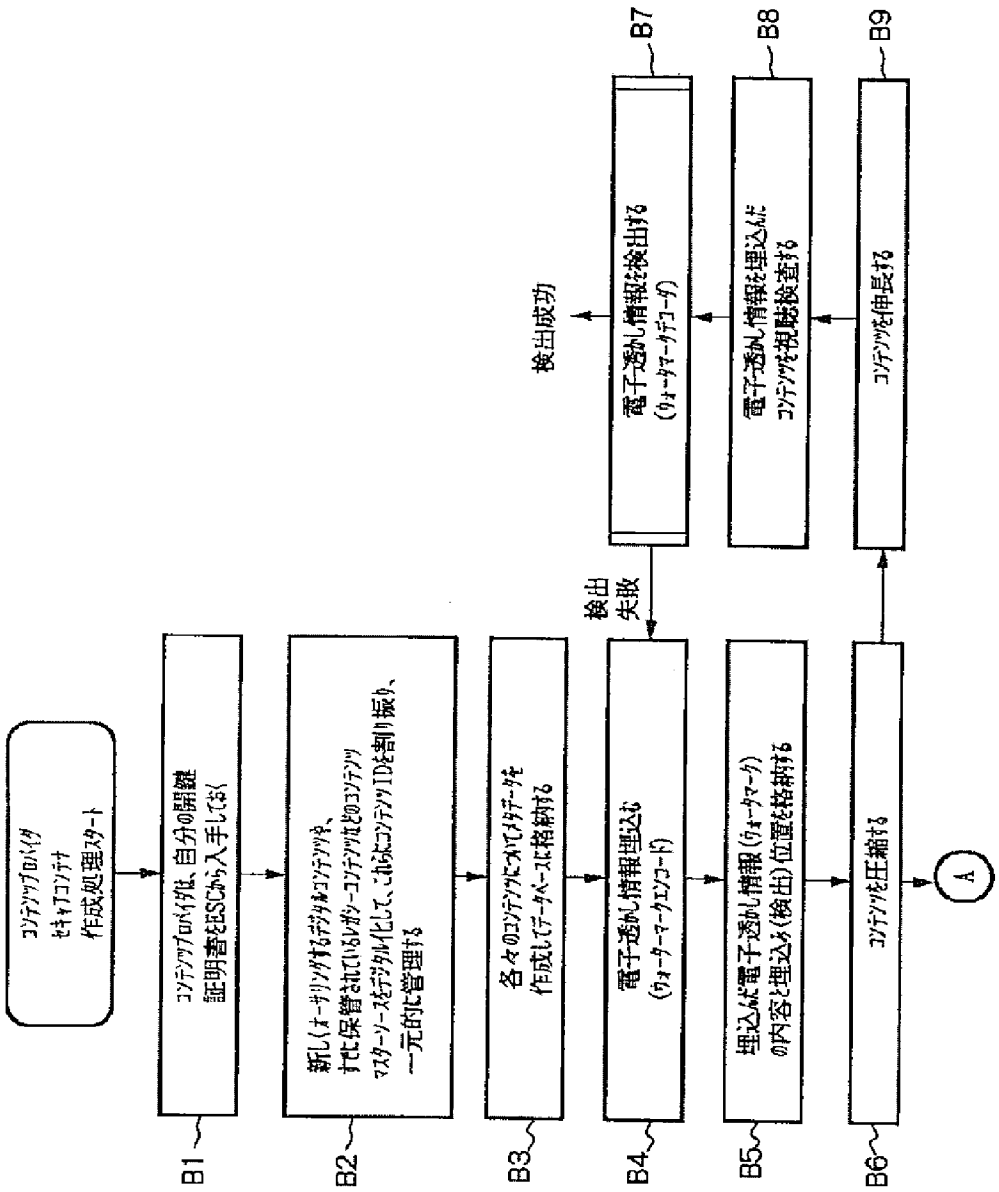
【図１９】


コンテンツプロバイダからEMD
サービスセンタへの登録処理スタート
A1
コンテンツプロバイダとEMDサービスセンタとの
間で相互認証を行う
認証失敗
認証成功
A2
セッション鍵を共有する
A3
登録を行う権利書データ等をデータ
ベースから読み出す
A4
権利書データに対し、コンテンツプロバイダの
秘密鍵を署名鍵として署名生成をおこない、署名を
含む登録用モジュールを作成
A5
登録用モジュールをセッション鍵で暗号化する
A6
登録用モジュールをEMDサービス
センタへ送信する
A7
EMDサービスセンタは受信した登録要求
モジュールをセッション鍵で復号化する
A8
EMDサービスセンタはコンテンツプロバイダの公開鍵を署名
検証鍵として、送られてきた登録モジュールに添付されている
署名データの署名検証をおこない、送り主の正当性の
証明をおこなう
署名検証
失敗
登録処理中止
署名検証成功
A9
権利書データ等をデータベースに登録する
登録処理終了

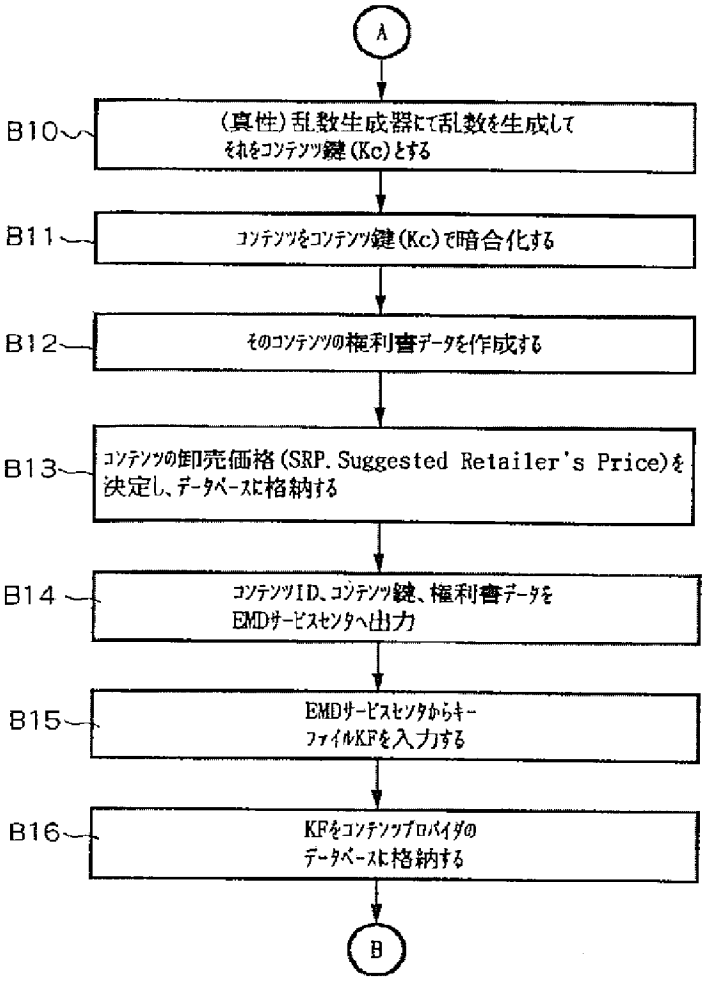
【図１１０】


310
コンテンツプロバイダ
決済(通知)
レポート
310
サービスプロバイダ
303a
303b
CA
SAM
1394
970
権利管理用
クリアリングハウス
971
電子決済用
クリアリングハウス
ペイメントゲートウェイ
90
利用明細書
少額決済
91
決済機関

【図２０】


コンテンツプロバイダ
セキュアコンテナ
作成処理スタート
B1
コンテンツプロバイダは、自分の開鍵
証明書をESCから入手しておく
B2
新しくオーサリングするデジタルコンテンツを、
すでに保管されているルボケーコンテンツなどのコンテンツ
マスターソースをデジタル化して、これらにコンテンツIDを割り振り、
一元的に管理する
B3
各々のコンテンツにメタデータを
作成してデータベース化格納する
B4
電子透かし情報埋込み
(ウォーターマークエンコード)
B5
埋込み電子透かし情報(ウォーターマーク)
の内容と埋込み(検出)位置を格納する
B6
コンテンツを圧縮する
A
検出失敗
検出成功
B7
電子透かし情報を検出する
(ウォーターマークデコード)
B8
電子透かし情報を埋込んだ
コンテンツを視聴検査する
B9
コンテンツを伸長する

【図２１】

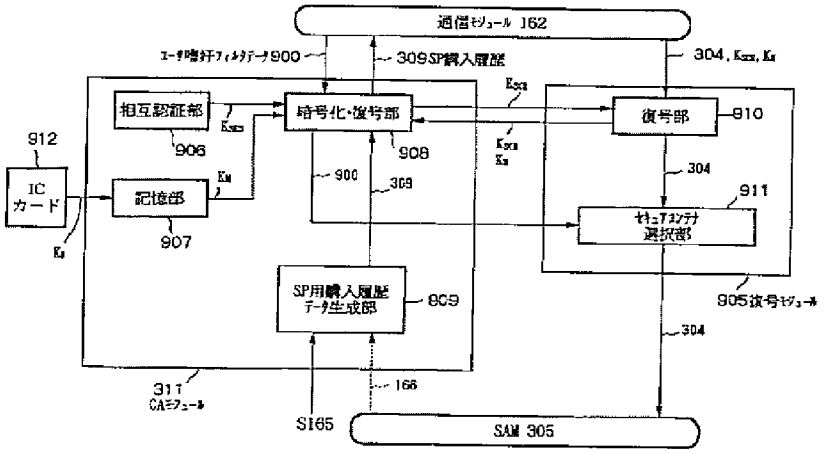


【図７３】

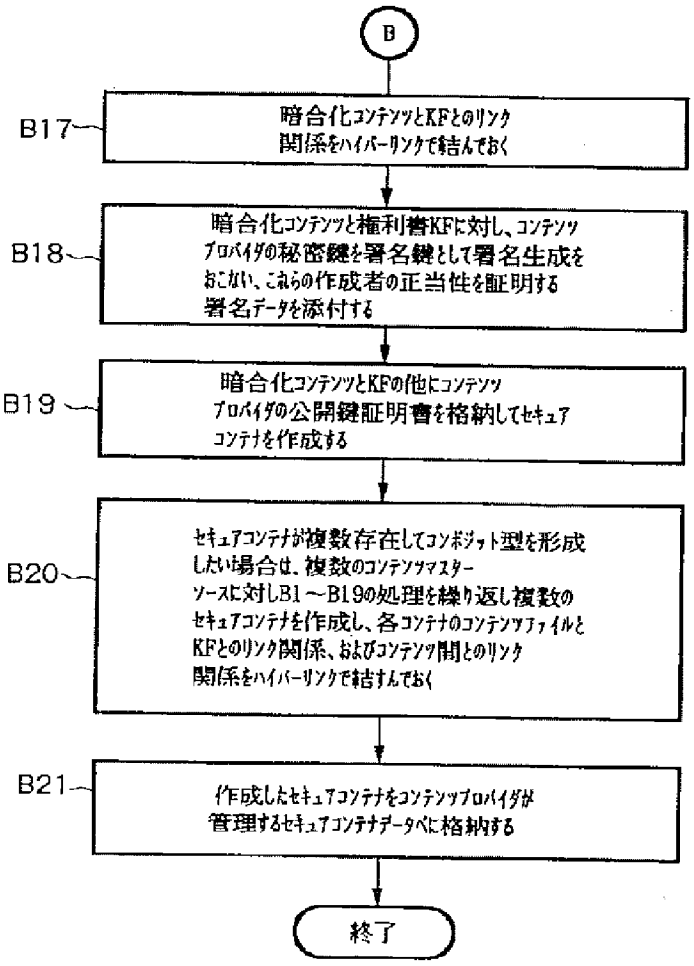
利用履歴データ308の内容

識別子Content_ID
識別子CP_ID
識別子SP_ID
コンテンツデータCの信号諸元データ
コンテンツデータCの圧縮方法
記録媒体の識別子Media_ID
識別子SAM_ID、
ユーザのUSER_ID

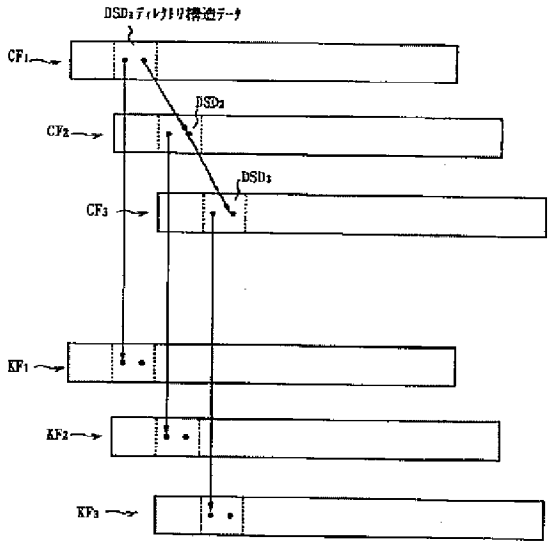
【図７５】



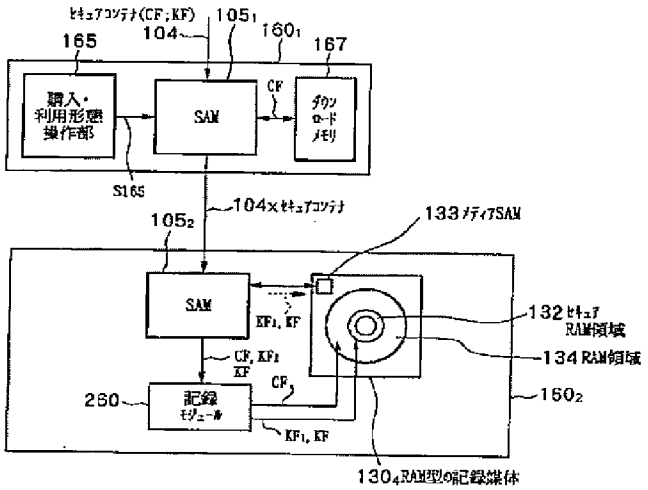
【図２２】


B
B17
暗合化コンテンツとKFとのリンク
関係をハイパーリンクで結んでおく
B18
暗合化コンテンツと権利書KFに対し、コンテンツ
プロバイダの秘密鍵を署名鍵として署名生成を
おこない、これらの作成者の正当性を証明する
署名データを添付する
B19
暗合化コンテンツとKFの他にコンテンツ
プロバイダの公開鍵証明書を格納してセキュア
コンテナを作成する
B20
セキュアコンテナが複数存在してコンポジット型を形成
したい場合は、複数のコンテンツマスター
ソースに対しB1～B19の処理を繰り返し複数の
セキュアコンテナを作成し、各コンテナのコンテンツファイルと
KFとのリンク関係、およびコンテンツ間とのリンク
関係をハイパーリンクで結んでおく
B21
作成したセキュアコンテナをコンテンツプロバイダが
管理するセキュアコンテナデータベに格納する
終了

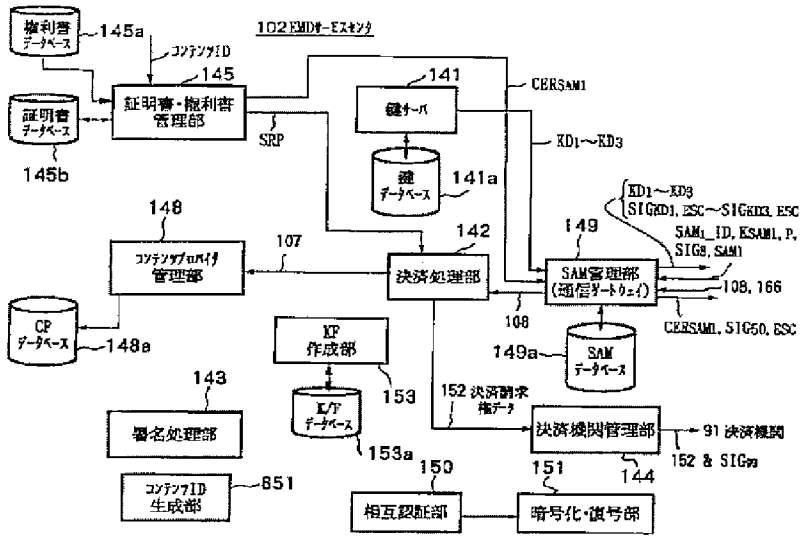
【図１１２】


DSD1 ディレクトリ構造データ
CF1
DSD2
CF2
DSD3
CF3
KF1
KF2
KF3

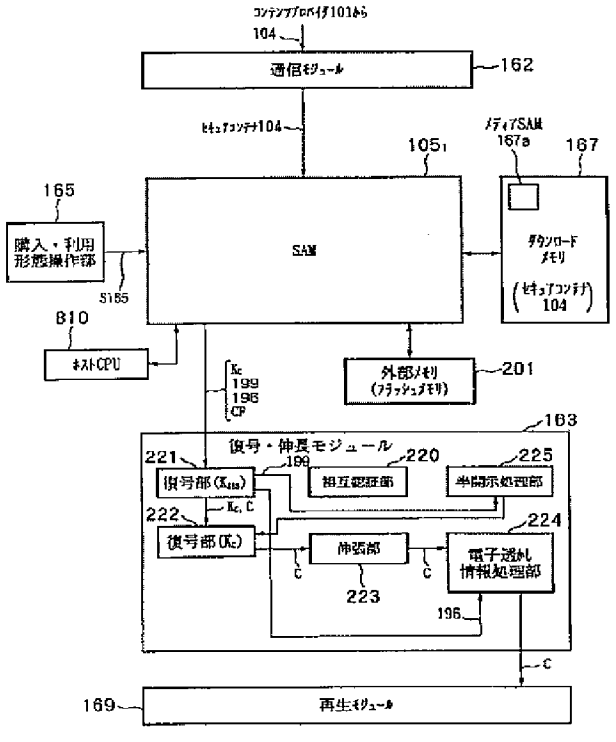
【図３２】


セキュアコンテナ(CF;KF)
165
104
105₁
160₁
167
購入・
利用形態
操作部
SAM
CF
ダウン
ロード
メモリ
S165
104×セキュアコンテナ
105₂
133 メディアSAM
SAM
KF1, KF
132 セキュア
RAM領域
134 RAM領域
CF, KF1
KF
260
記録
モジュール
CF2
160₂
KF1, KF
130 RAM型の記録媒体

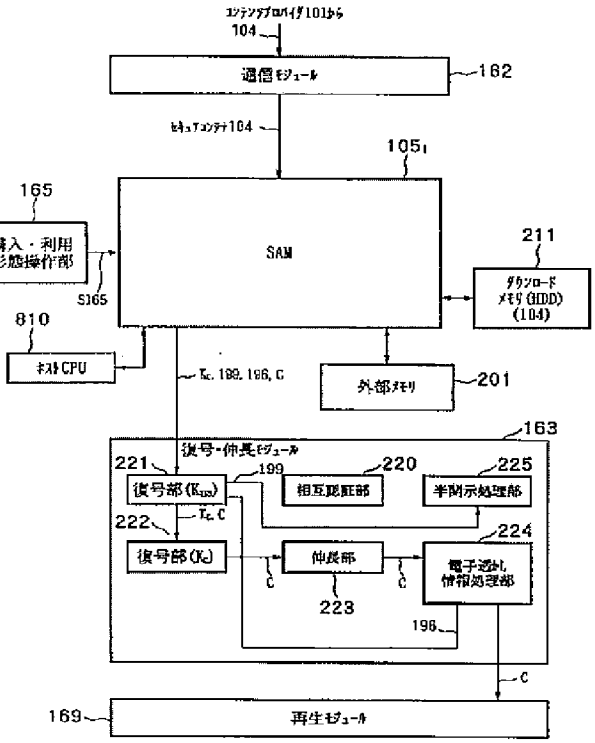
【図２４】


権利書データベース
145a
コンテンツID
102 EMDサービスセンタ
145
証明書・権利書管理部
証明書データベース
145b
SRP
141
鍵サーバ
CERSAM1
KD1～KD3
鍵データベース
141a
148
コンテンツプロバイダ管理部
107
142
決済処理部
149
SAM管理部（通信ゲートウェイ）
KD1～KD3
SIGKD1, ESC～SIGKD3, ESC
SAM1_ID, ESAM1, P, SIG8, SAM1
108, 166
CERSAM1, SIG50, ESC
108
CPデータベース
148a
KF作成部
149a
SAMデータベース
153
KF/Fデータベース
153a
143
署名処理部
152 決済請求権データ
決済機関管理部
91 決済機関
152 & SIG99
150
151
144
コンテンツID生成部
851
相互認証部
暗号化・復号部

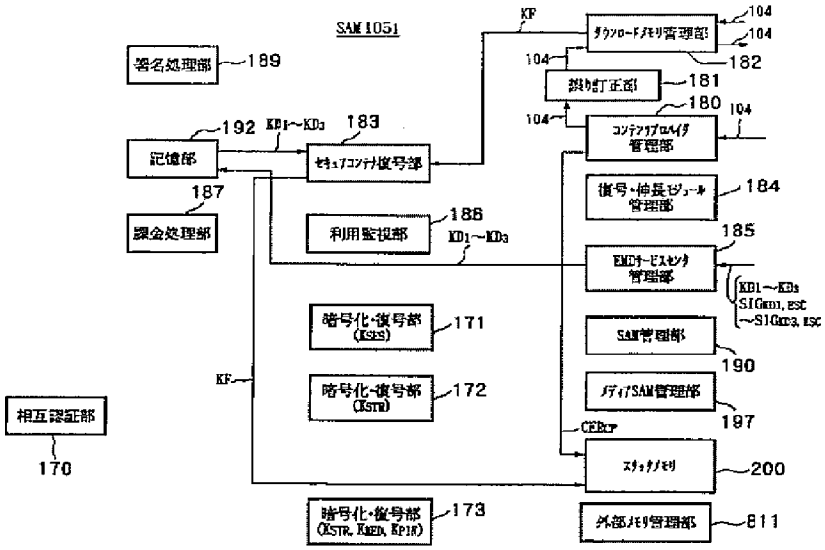
【図２５】


コンテンツプロバイダ101から
104
通信モジュール
162
セキュアコンテナ104
105₁
メディアSAM 167a
167
165
購入・利用形態操作部
SAM
ダウンロードメモリ
（セキュアコンテナ104）
S165
810
ホストCPU
Kc 199 196 CP
外部メモリ（フラッシュメモリ）
201
163
復号・伸長モジュール
221
199
220
225
復号部（K_{title}）
相互認証部
半開示処理部
222
Kc, C
復号部（Kc）
伸張部
224
電子透かし情報処理部
C
223
196
169
再生モジュール

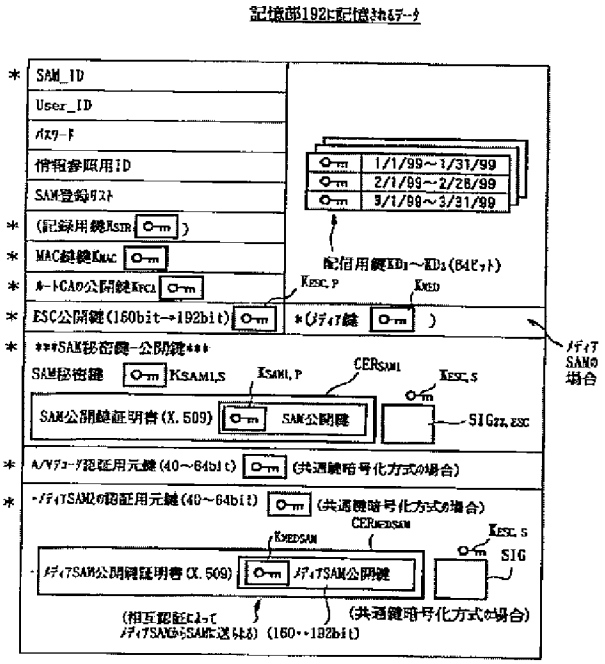
【図２９】


コンテンツプロバイダ101から
104
通信モジュール
162
セキュアコンテナ104
105₁
165
購入・利用形態操作部
SAM
211
ダウンロードメモリ（HDD）（104）
S165
810
ホストCPU
Kc, 199, 196, C
外部メモリ
201
163
復号・伸長モジュール
221
199
220
225
復号部（K_{title}）
相互認証部
半開示処理部
222
Kc, C
復号部（Kc）
伸長部
224
電子透かし情報処理部
C
223
196
169
再生モジュール

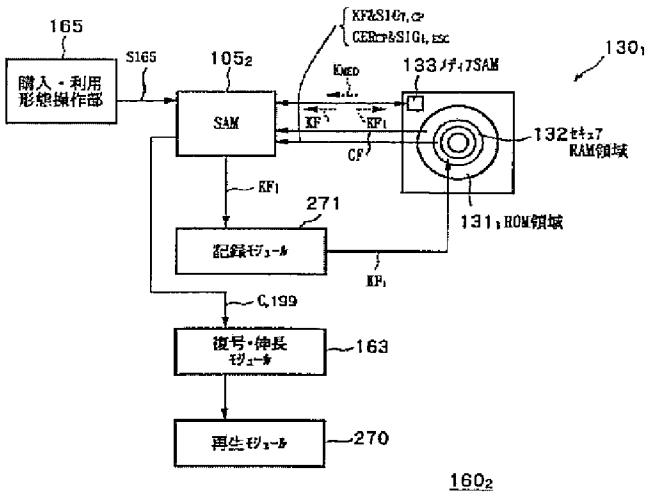
【図２６】


SAM 1051
署名処理部
189
記憶部
192
KD1～KD3
183
セキュアコンテナ復号部
187
課金処理部
利用監視部
186
KD1～KD3
暗号化・復号部
(KSES)
171
暗号化・復号部
(KSTR)
172
相互認証部
170
KF
ダウンロードメモリ管理部
104
104
182
誤り訂正部
181
104
コンテンツプロバイダ管理部
180
104
復号・伸長モジュール管理部
184
185
EMDサービスセンタ管理部
KD1～KD3
SIGKD1, ESC
～SIGKD3, ESC
SAM管理部
190
メディアSAM管理部
197
CERCP
スチャノメモリ
200
暗号化・復号部
(KSTR, KMED, KP1R)
173
外部メモリ管理部
811

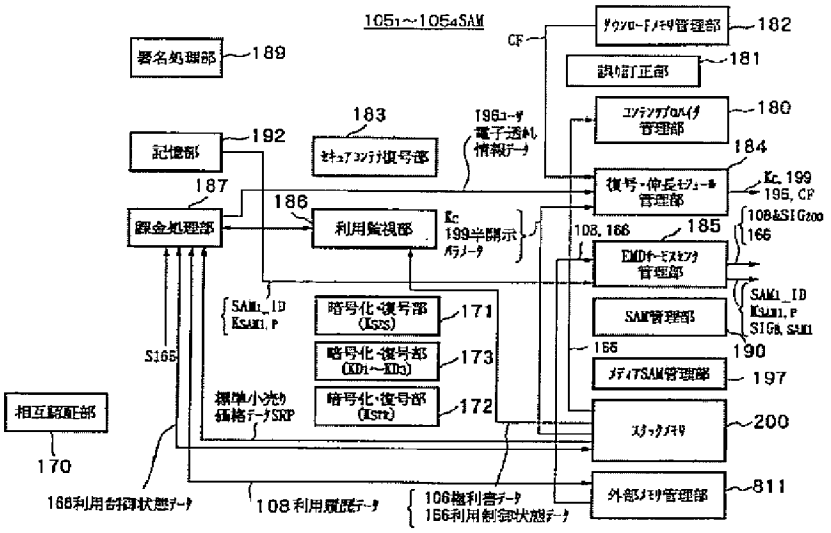
【図３０】


記憶部192に記憶されるデータ
SAM_ID
User_ID
パスワード
情報参照用ID
SAM登録リスト
(記録用鍵KSTR)
MAC鍵KMAC
A-TCAの公開鍵KPCA
ESC公開鍵(160bit→192bit)
1/1/99～1/31/99
2/1/99～2/28/99
3/1/99～3/31/99
配信用鍵KD1～KD3(64ビット)
KESC, P
KMED
*(メディア鍵
)
メディアSAMの場合
SAM秘密鍵-公開鍵
SAM秘密鍵
KSAM1, S
KSAM1, P
CERSAM1
KESC, S
SAM公開鍵証明書(X.509)
SAM公開鍵
SIGSAM, ESC
A/Vデコード認証用元鍵(40～64bit)
(共通鍵暗号化方式の場合)
メディアSAMの認証用元鍵(40～64bit)
(共通鍵暗号化方式の場合)
CERMEDSAM
KMEDSAM
KESC, S
SIG
メディアSAM公開鍵証明書(X.509)
メディアSAM公開鍵
(相互認証によってメディアSAMからSAMに送られる)
(160→192bit)
(共通鍵暗号化方式以外)

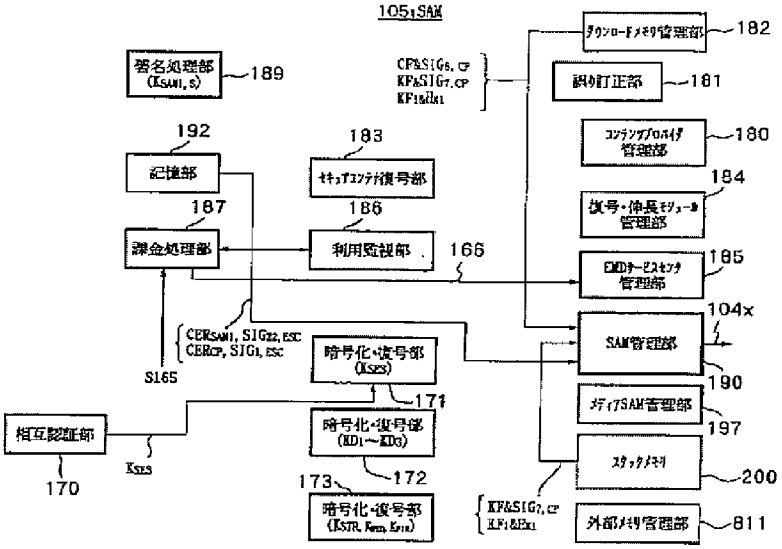
【図３６】


165
購入・利用形態操作部
S165
105₂
SAM
KF&SIG1, CP
CERCP&SIG1, ESC
KMED
133メディアSAM
130₁
KF
KP1
CP
132セキュアRAM領域
131₁ ROM領域
KF1
271
記録モジュール
KP1
C, 199
復号・伸長モジュール
163
再生モジュール
270
160₂

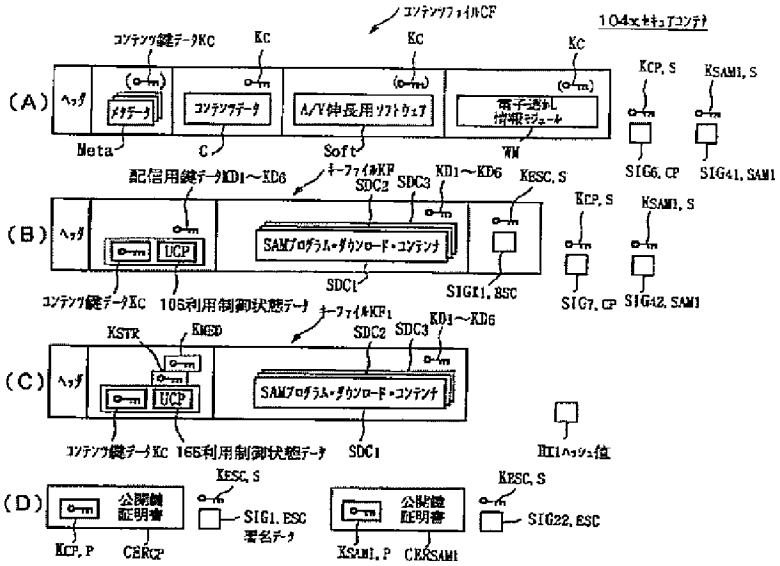
【図３１】


105₁～105ₐSAM
署名処理部
189
CF
ダウンロードメモリ管理部
182
誤り訂正部
181
コンテンツプロバイダ管理部
180
記憶部
192
セキュアコンテナ復号部
183
198ユーザ電子透かし情報データ
184
復号・伸長モジュール管理部
Kc, 199
195, CP
187
課金処理部
186
利用監視部
Kc
199半開示パラメータ
108, 166
185
EMDサービスセンタ管理部
108&SIG200
165
SAM1_ID
KSAM1, P
暗号化・復号部
(KSES)
171
SAM管理部
SAM1_ID
KSAM1, P
SIG8, SAM1
190
S165
暗号化・復号部
(KD1～KDn)
173
166
メディアSAM管理部
197
標準小売り価格データSKP
暗号化・復号部
(KSTR)
172
スタックメモリ
200
相互認証部
170
166利用制御状態データ
108利用履歴データ
106権利書データ
166利用制御状態データ
外部メモリ管理部
811

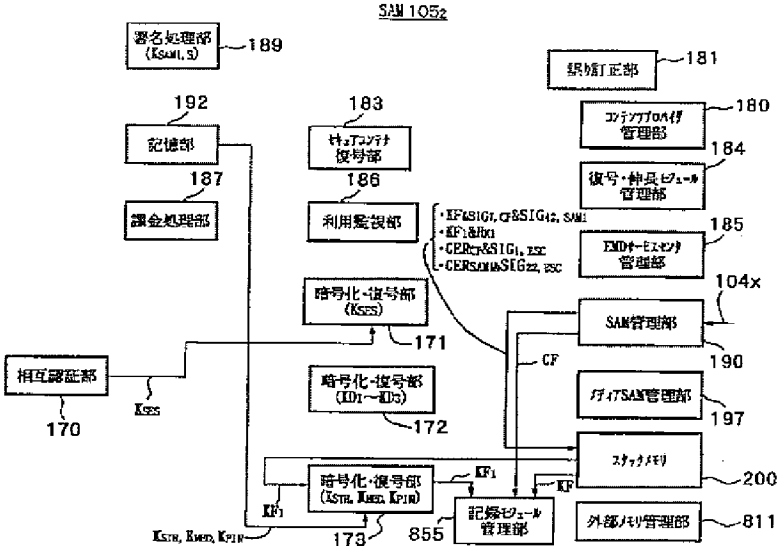
【図３３】


105₁SAM
署名処理部
(KSAM1, S)
189
CP&SIG6, CP
KP&SIG7, CP
KF1&Ek1
ダウンロードメモリ管理部
182
誤り訂正部
181
コンテンツプロバイダ管理部
180
192
記憶部
183
セキュアコンテナ復号部
184
復号・伸長モジュール管理部
187
課金処理部
186
利用監視部
166
185
EMDサービスセンタ管理部
104x
CERSAM1, SIG22, ESC
CERCP, SIG1, ESC
暗号化・復号部
(KSES)
SAM管理部
190
S165
171
メディアSAM管理部
197
暗号化・復号部
(KD1～KDn)
相互認証部
KSES
スタックメモリ
200
170
173
暗号化・復号部
(KSTR, Km, Ek12)
172
KF&SIG7, CP
KF1&Ek1
外部メモリ管理部
811

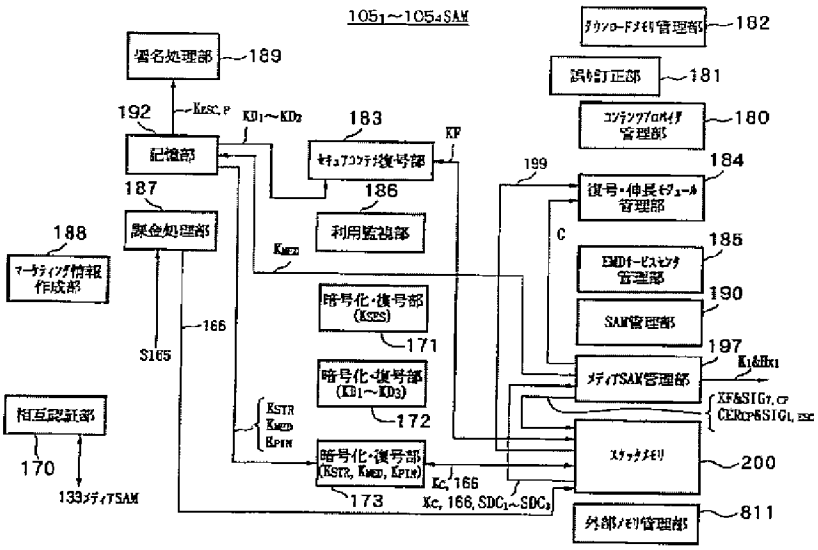
【図３４】


(A)
(B)
(C)
(D)
Meta
C
Soft
WM
SAMプログラム・ダウンロード・コンテンツ
UCP
SDC1
SDC2
SDC3
KD1～KD6
KSTR
KMED
KCP, P
CERCP
KSAM1, P
CERSAM1
SIG1, ESC
SIG22, ESC
SIG6, CP
SIG41, SAM1
SIG7, CP
SIG42, SAM1
H1ハッシュ値

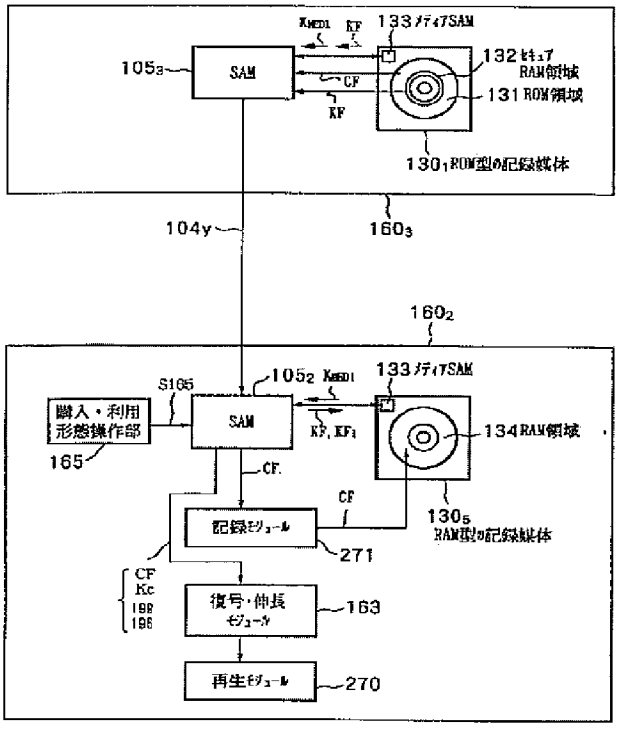
【図３５】


SAM 105₂
署名処理部
189
192
記憶部
187
課金処理部
183
セキュアコンテナ復号部
186
利用監視部
171
暗号化・復号部
(KSES)
172
暗号化・復号部
(KD1～KD6)
170
相互認証部
KSES
173
KSTR, KMED, KP1R
855
記録ビュー管理部
181
180
184
185
104x
190
197
200
811
CF
KF1
KF
SAM管理部
外部メモリ管理部

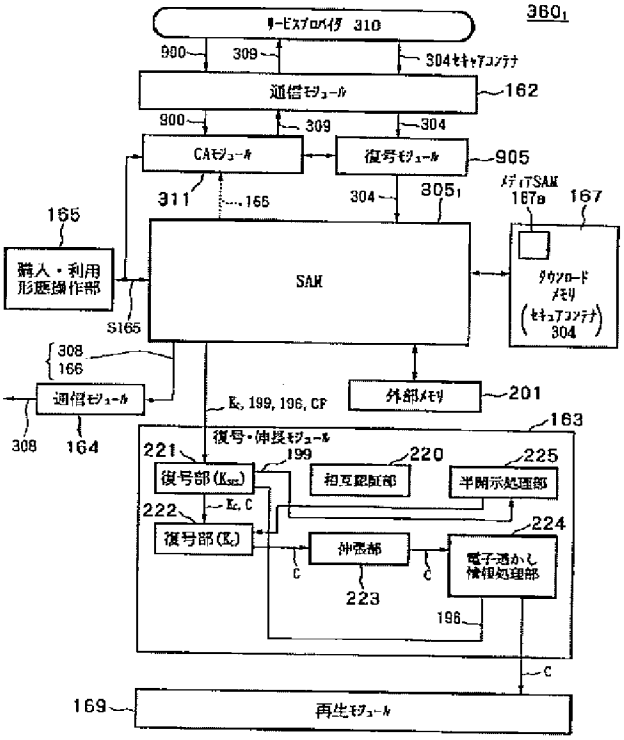
【図３７】


105₁～105₄SAM
署名処理部
189
192
記憶部
183
186
利用監視部
187
課金処理部
188
マーケティング情報作成部
暗号化・復号部(KSES)
171
暗号化・復号部(KD1～KD3)
172
暗号化・復号部(KSTR, KMED, KPIN)
173
相互認証部
170
133メディアSAM
166
S165
199
C
ダウンロードメモリ管理部
182
誤り訂正部
181
コンテンツプロバイダ管理部
180
184
復号・伸長モジュール管理部
185
EMDサービスセンタ管理部
190
SAM管理部
197
メディアSAM管理部
スタックメモリ
200
外部メモリ管理部
811
Kc, 166, SDC₁～SDC₃

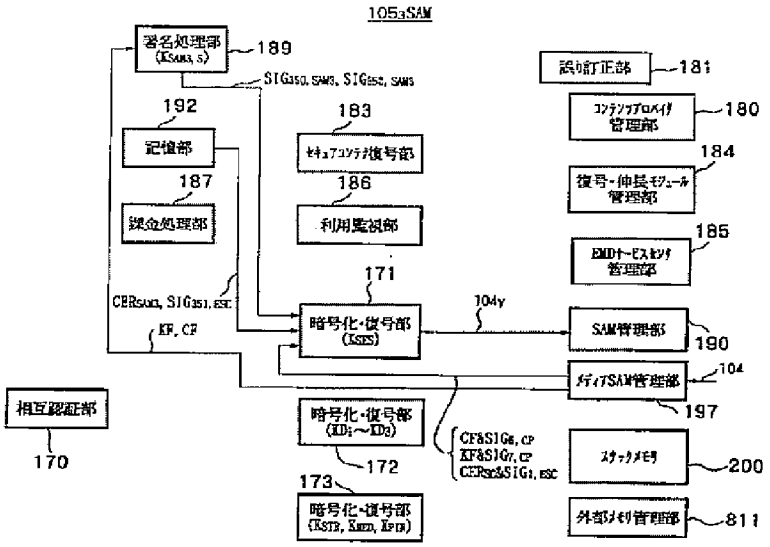
【図３８】


105₃
SAM
133メディアSAM
132セキュアRAM領域
131 ROM領域
130₁ROM型の記録媒体
160₃
104y
160₂
105₂
134RAM領域
130₅RAM型の記録媒体
購入・利用形態操作部
165
S165
記録モジュール
271
復号・伸長モジュール
163
再生モジュール
270

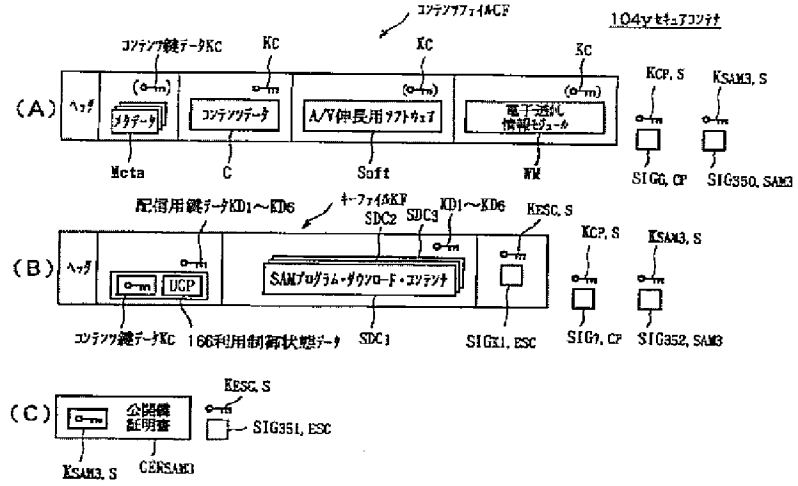
【図７４】


360₁
サービスプロバイダ 310
通信モジュール
162
CAモジュール
復号モジュール
905
305₁
メディアSAM 167a
167
ダウンロードメモリ(セキュアコンテナ)304
SAM
165
購入・利用形態操作部
S165
通信モジュール
164
外部メモリ
201
163
復号・伸長モジュール
復号部(Kscr)
相互認証部
220
225
半開示処理部
復号部(Kc)
伸張部
223
224
電子透かし情報処理部
196
再生モジュール
169

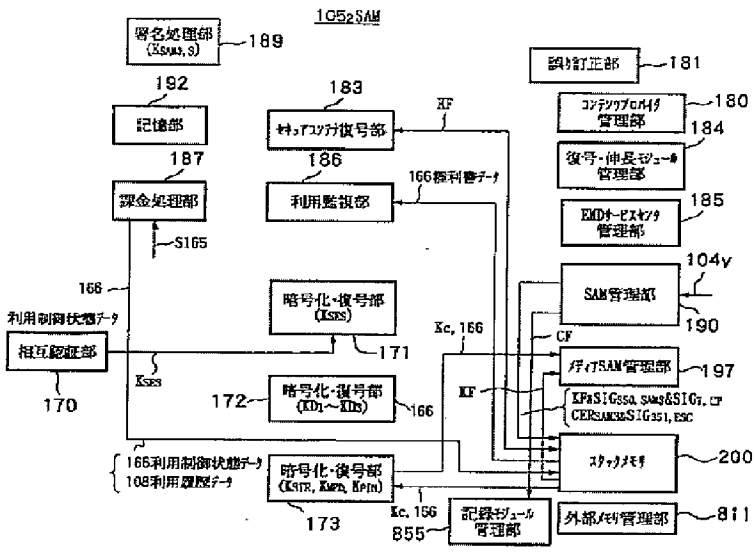
【図３９】


105a SAM
署名処理部
189
誤り訂正部
181
192
183
180
記憶部
187
186
184
課金処理部
利用監視部
185
171
104y
190
104
197
相互認証部
170
172
173
200
811

【図４０】

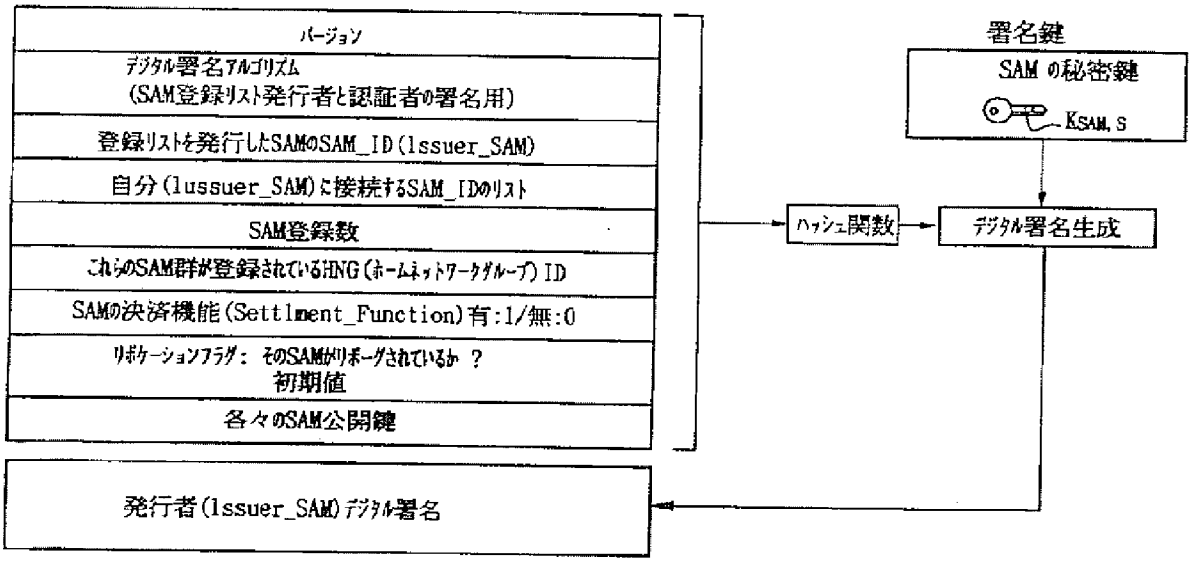

(A)
(B)
(C)
Meta
C
Soft
SIG6, CP
SIG350, SAM3
SIG1, ESC
SIG7, CP
SIG352, SAM3
SIG351, ESC

【図４１】

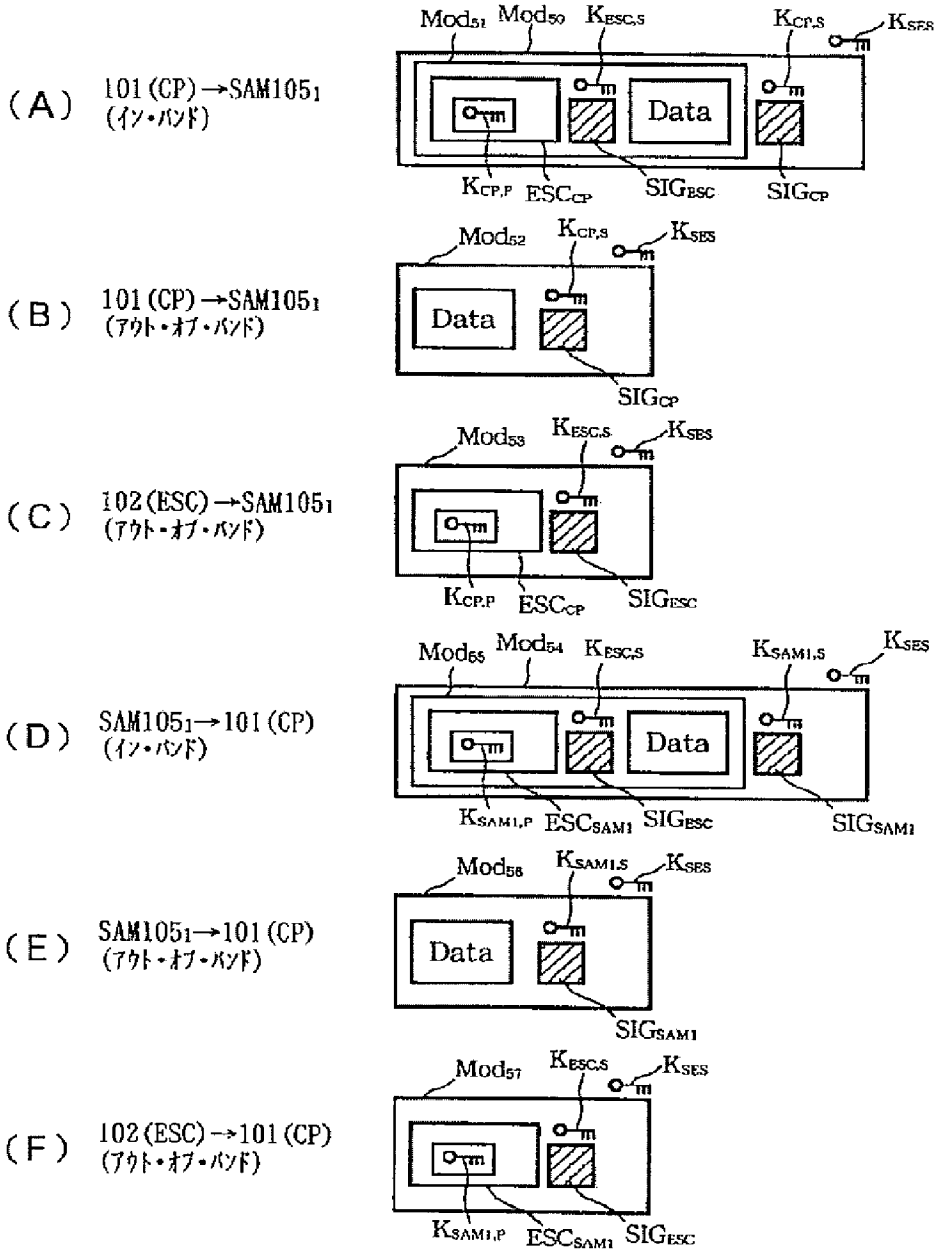


【図４５】

SAM登録リスト(SAM Registration List)(SAMが作成)

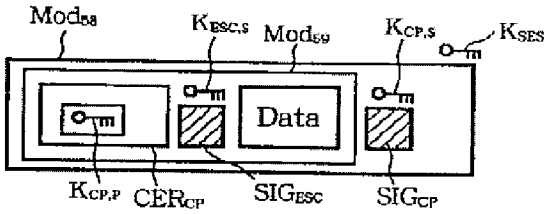


【図４２】

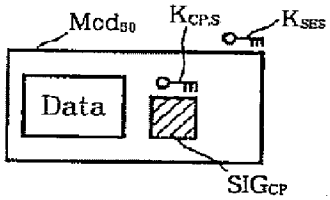

(A) 101(CP)→SAM105₁
(イン・バンド)
Mod51 Mod50 KESC,S KCP,S KSES
Data
KCP,P ESCCP SIGESC SIGCP
(B) 101(CP)→SAM105₁
(アウト・オブ・バンド)
Mod52 KCP,S KSES
Data
SIGCP
(C) 102(ESC)→SAM105₁
(アウト・オブ・バンド)
Mod53 KESC,S KSES
KCP,P ESCCP SIGESC
(D) SAM105₁→101(CP)
(イン・バンド)
Mod55 Mod54 KESC,S KSAM1,S KSES
Data
KSAM1,P ESCSAM1 SIGESC SIGSAM1
(E) SAM105₁→101(CP)
(アウト・オブ・バンド)
Mod56 KSAM1,S KSES
Data
SIGSAM1
(F) 102(ESC)→101(CP)
(アウト・オブ・バンド)
Mod57 KESC,S KSES
KSAM1,P ESCSAM1 SIGESC

【図４３】

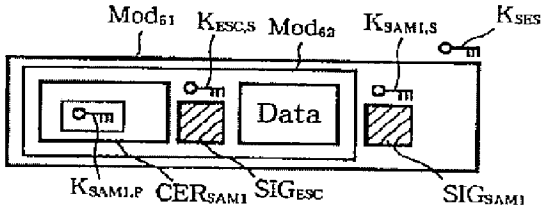
（G）　101(CP)→102(ESC)
(イン・バンド)



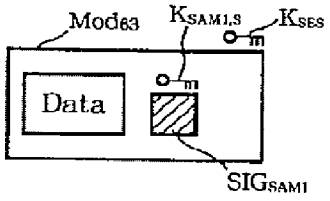
（H）　101(CP)→102(ESC)
(アウト・オブ・バンド)



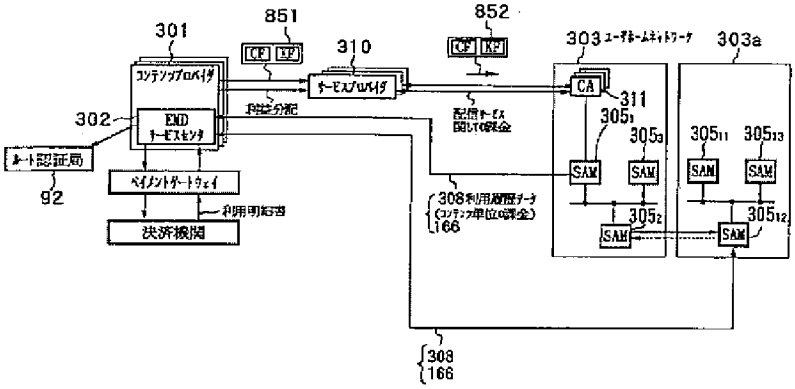
（I）　SAM105$_1$→102(ESC)
(イン・バンド)



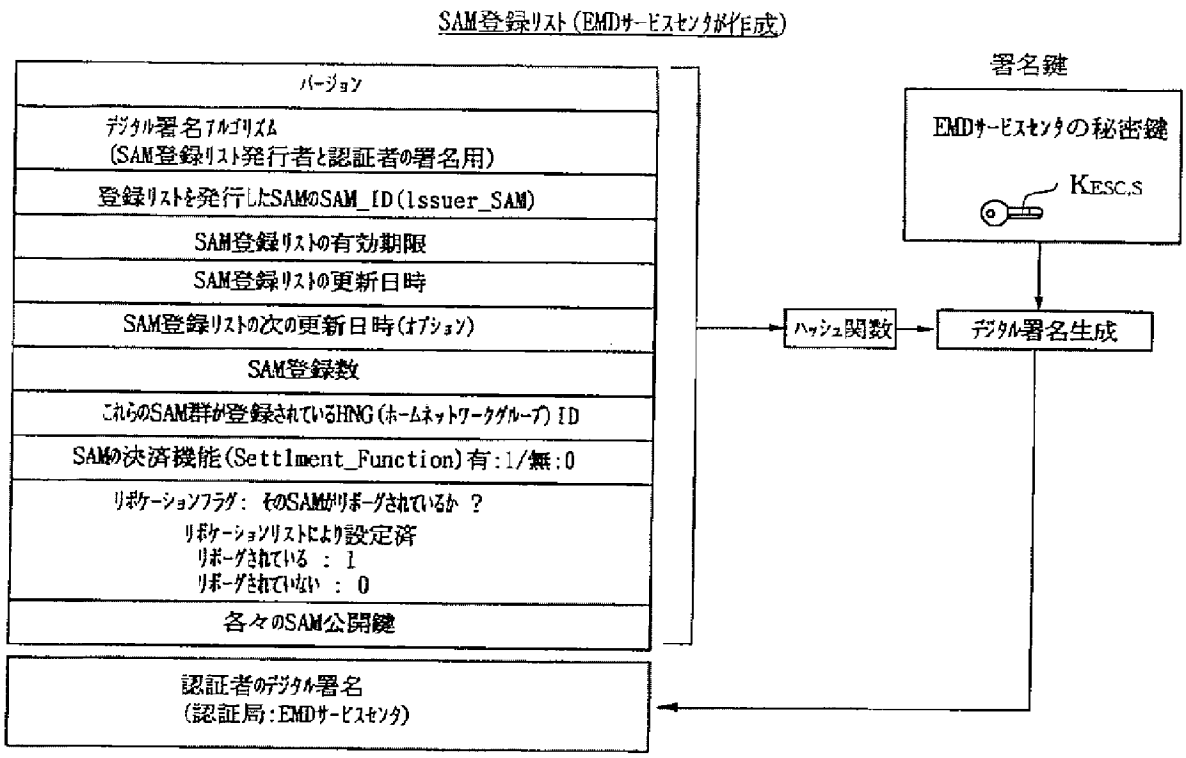
（J）　SAM105$_1$→102(ESC)
(アウト・オブ・バンド)



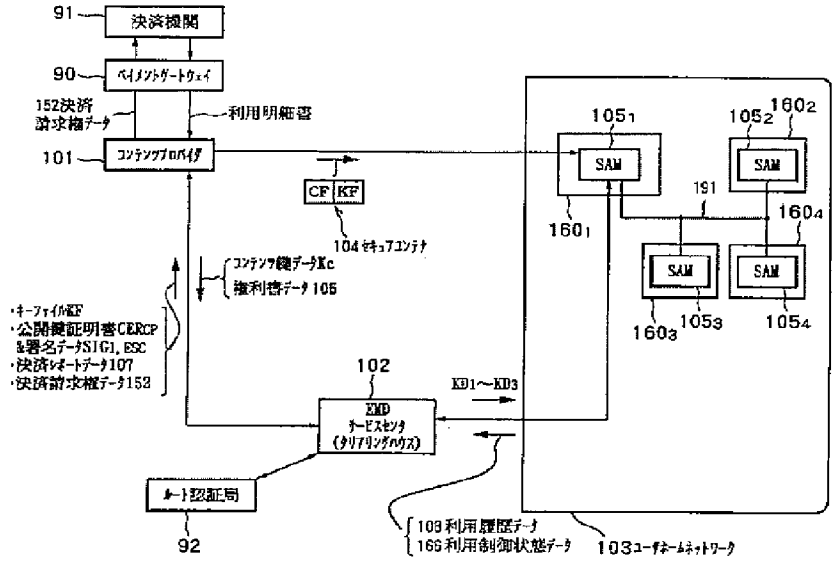
【図１４３】



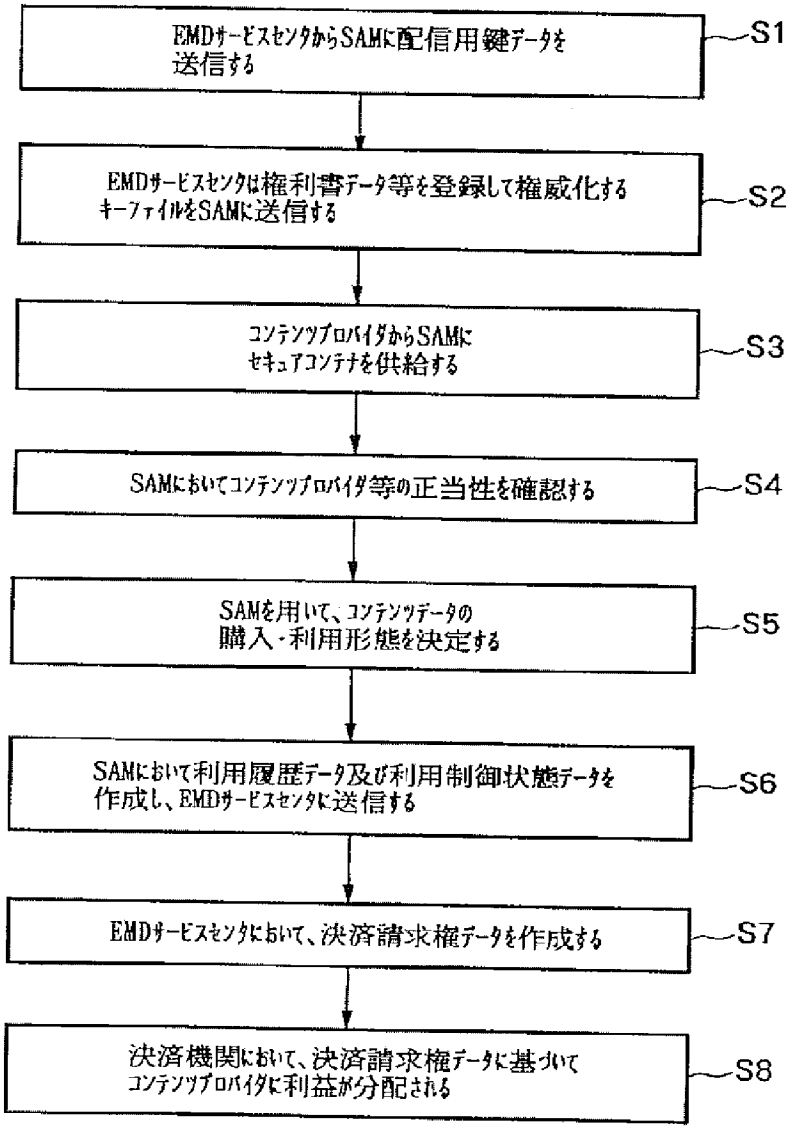
【図４６】


SAM登録リスト（EMDサービスセンタが作成）
バージョン
デジタル署名アルゴリズム
（SAM登録リスト発行者と認証者の署名用）
登録リストを発行したSAMのSAM_ID（Issuer_SAM）
SAM登録リストの有効期限
SAM登録リストの更新日時
SAM登録リストの次の更新日時（オプション）
SAM登録数
これらのSAM群が登録されているHNG（ホームネットワークグループ）ID
SAMの決済機能（Settlment_Function）有：1/無：0
リボケーションフラグ：そのSAMがリボークされているか ？
リボケーションリストにより設定済
リボークされている ： 1
リボークされていない ： 0
各々のSAM公開鍵
認証者のデジタル署名
（認証局：EMDサービスセンタ）
署名鍵
EMDサービスセンタの秘密鍵
KESC,S
ハッシュ関数
デジタル署名生成

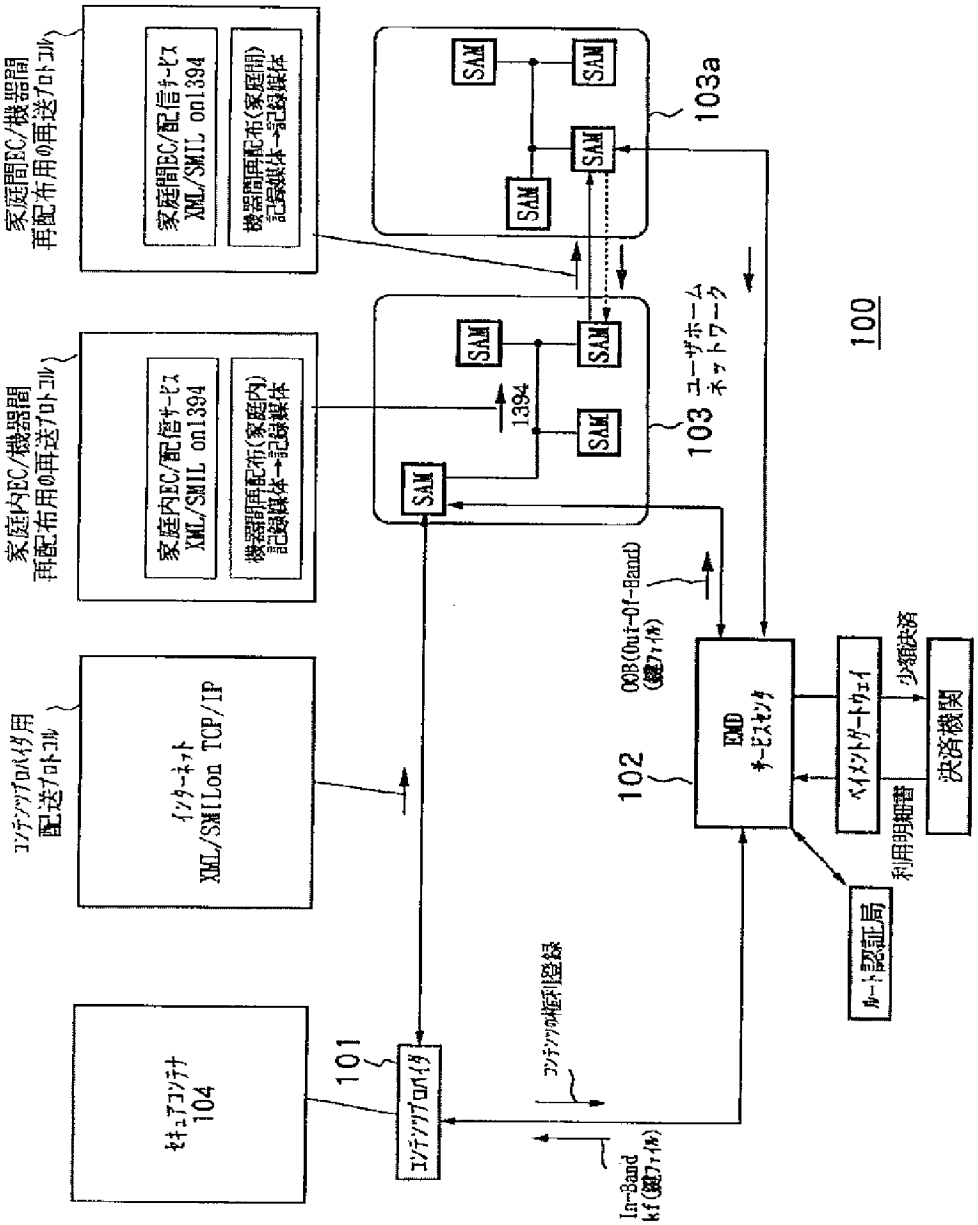
【図４９】


91
決済機関
90
ペイメントゲートウェイ
152決済請求権データ
利用明細書
101
コンテンツプロバイダ
CF
KF
104 セキュアコンテナ
コンテンツ鍵データKc
権利情データ 105
・キーファイルKF
・公開鍵証明書CERCP
&署名データSIG1, ESC
・決済レポートデータ107
・決済請求権データ152
102
EMD
サービスセンタ
（クリアリングハウス）
KD1～KD3
ルート認証局
92
103利用履歴データ
166利用制御状態データ
103ユーザホームネットワーク
SAM
1051
1052
1602
1601
191
1604
1603
1053
1054

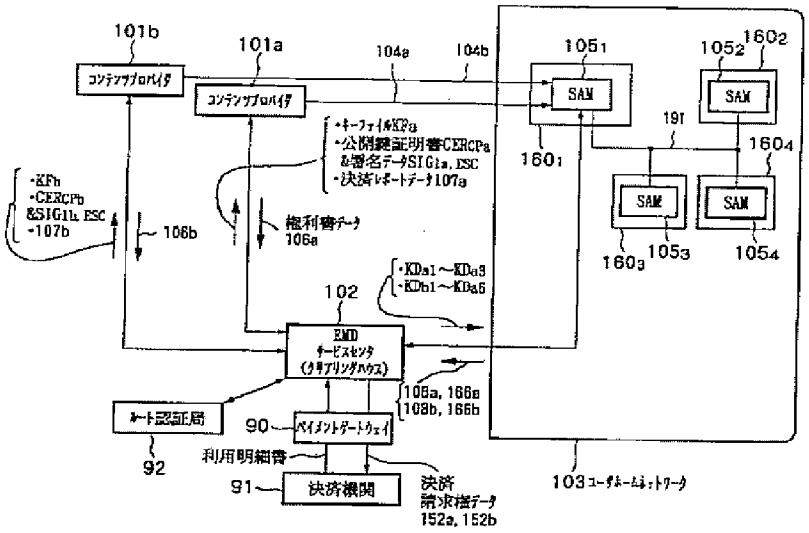
【図４７】


EMDサービスセンタからSAMに配信用鍵データを送信する
S1
EMDサービスセンタは権利書データ等を登録して権威化するキーファイルをSAMに送信する
S2
コンテンツプロバイダからSAMにセキュアコンテナを供給する
S3
SAMにおいてコンテンツプロバイダ等の正当性を確認する
S4
SAMを用いて、コンテンツデータの購入・利用形態を決定する
S5
SAMにおいて利用履歴データ及び利用制御状態データを作成し、EMDサービスセンタに送信する
S6
EMDサービスセンタにおいて、決済請求権データを作成する
S7
決済機関において、決済請求権データに基づいてコンテンツプロバイダに利益が分配される
S8

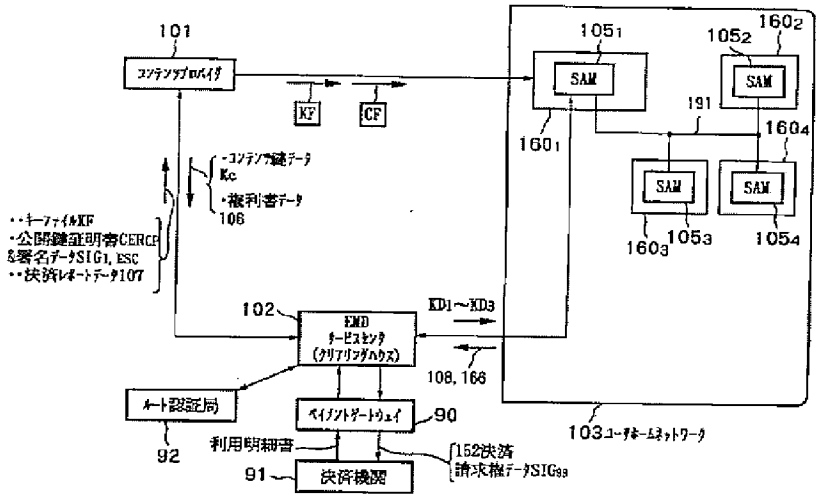
【図４８】


家庭間EC/機器間
再配布用の再送プロトコル
家庭間EC/配信サービス
XML/SMIL on1394
機器間再配布(家庭間)
記録媒体→記録媒体
家庭内EC/機器間
再配布用の再送プロトコル
家庭内EC/配信サービス
XML/SMIL on1394
機器間再配布(家庭内)
記録媒体→記録媒体
コンテンツプロバイダ用
配送プロトコル
インターネット
XML/SMILon TCP/IP
セキュアコンテナ
104
101
コンテンツプロバイダ
コンテンツの権利登録
In-Band
kf(鍵ファイル)
SAM
1394
103
ユーザホーム
ネットワーク
103a
100
OOB(Out-Of-Band)
(鍵ファイル)
102
EMD
サービスセンタ
ペイメントゲートウェイ
少額決済
決済機関
利用明細書
ルート認証局

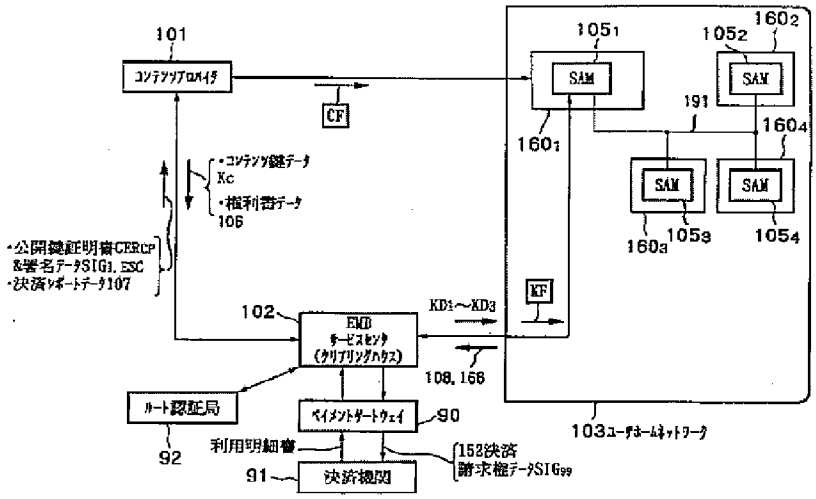
【図５０】


101b
101a
104a
104b
1051
1052
1602
SAM
SAM
191
1601
1604
SAM
SAM
1603
1053
1054
・KFh
・CERCPb
&SIG1b, ESC
・107b
106b
権利書データ
106a
・キーファイルKFa
・公開鍵証明書CERCPa
&署名データSIG1a, ESC
・決済レポートデータ107a
・KDa1～KDa3
・KDb1～KDa6
102
EMD
サービスセンタ
(クリアリングハウス)
108a, 166a
108b, 166b
カード認証局
90
ペイメントゲートウェイ
92
利用明細書
91
決済機関
決済
請求権データ
152a, 152b
103ユーザホームネットワーク

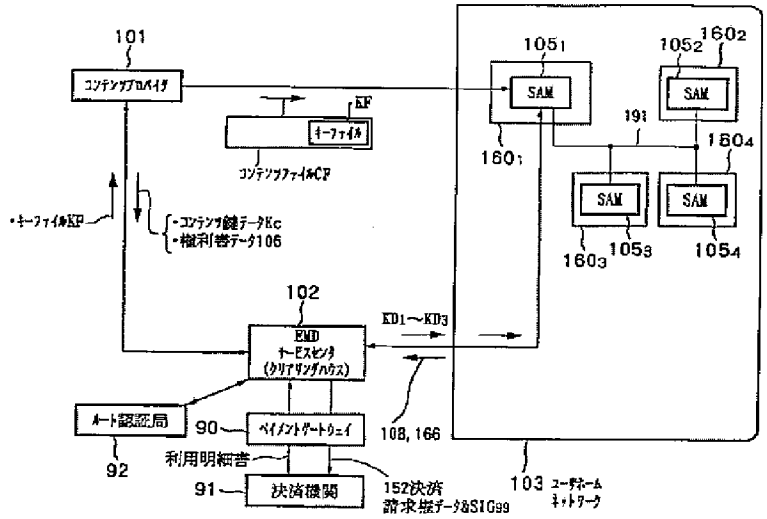
【図５１】


101
コンテンツプロバイダ
KF
CF
1051
1052
1602
SAM
SAM
191
1601
1604
SAM
SAM
1603
1053
1054
・コンテンツ鍵データ
Kc
・権利書データ
106
・キーファイルKF
・公開鍵証明書CERCF
&署名データSIG1, ESC
・決済レポートデータ107
102
EMD
サービスセンタ
(クリアリングハウス)
KD1～KD3
108, 166
カード認証局
ペイメントゲートウェイ
90
92
利用明細書
152決済
請求権データSIG93
91
決済機関
103ユーザホームネットワーク

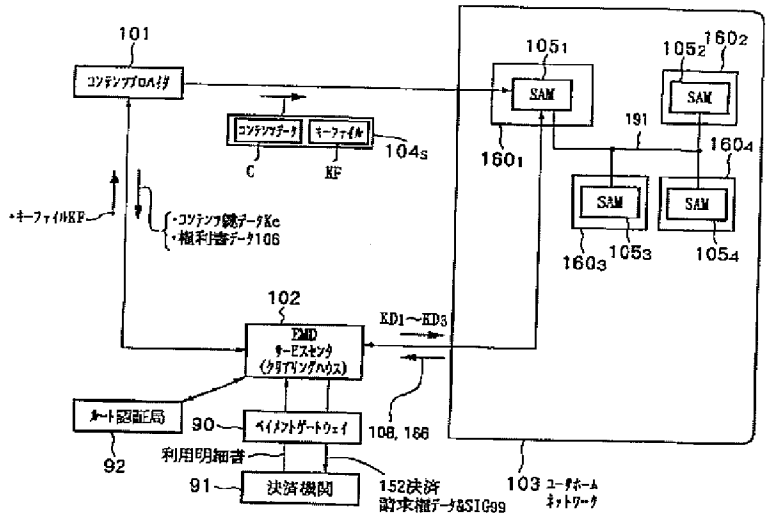
【図５２】


101
コンテンツプロバイダ
CF
・コンテンツ鍵データ Kc
・権利書データ 106
・公開鍵証明書CERCP &署名データSIG1, ESC
・決済レポートデータ107
102
EMD サービスセンタ (クリアリングハウス)
KD1～KD3
108, 166
KF
ルート認証局
92
ペイメントゲートウェイ
90
利用明細書
91
決済機関
152決済 請求書データSIG99
1051
1052
1602
SAM
191
1601
1604
1603
1053
1054
103ユーザホームネットワーク

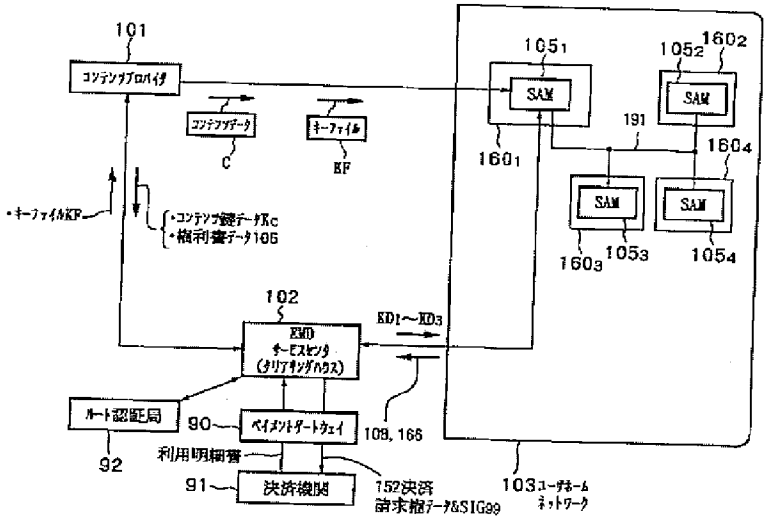
【図５３】


101
コンテンツプロバイダ
KF
キーファイル
コンテンツファイルCP
・キーファイルKP
・コンテンツ鍵データKc
・権利書データ106
102
EMD サービスセンタ (クリアリングハウス)
KD1～KD3
108, 166
ルート認証局
92
ペイメントゲートウェイ
90
利用明細書
91
決済機関
152決済 請求書データ&SIG99
1051
1052
1602
SAM
191
1601
1604
1603
1053
1054
103 ユーザホーム ネットワーク

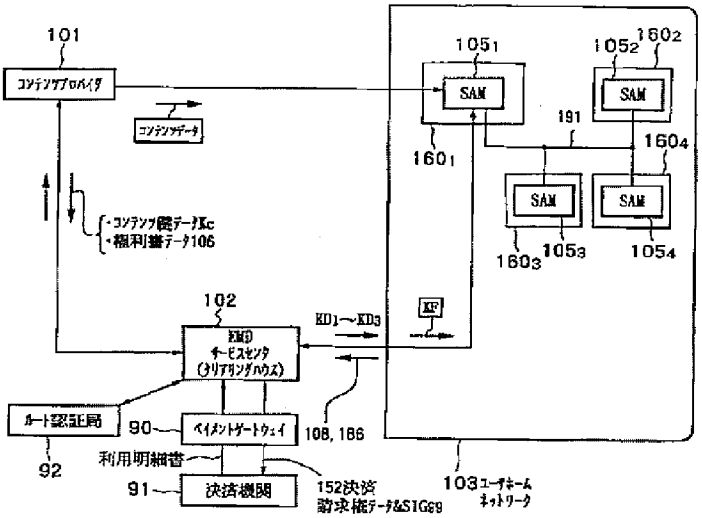
【図５４】


101
コンテンツプロバイダ
コンテンツデータ
キーファイル
C
KF
104s
・キーファイルKF
・コンテンツ鍵データKc
・権利書データ106
1051
SAM
1601
1052
1602
SAM
191
1604
SAM
SAM
1603
1053
1054
102
EMD
サービスセンタ
(クリアリングハウス)
KD1～KD3
カード認証局
90
ペイメントゲートウェイ
108, 166
92
利用明細書
91
決済機関
152決済
請求権データ&SIG99
103 ユーザホーム
ネットワーク

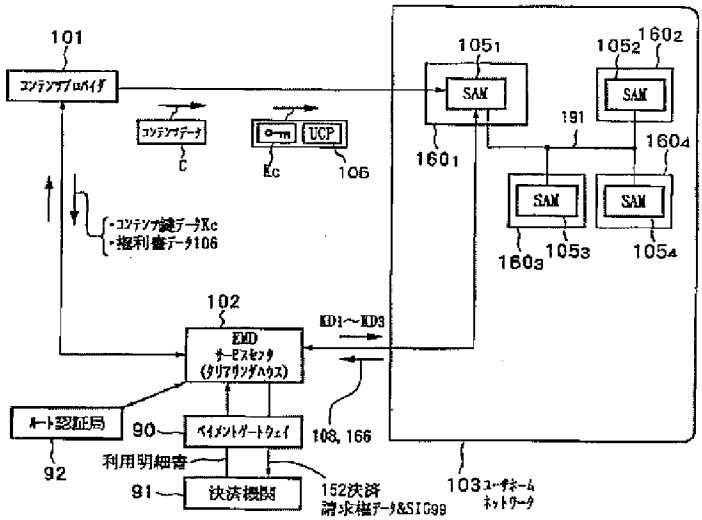
【図５５】


101
コンテンツプロバイダ
コンテンツデータ
キーファイル
C
KF
・キーファイルKF
・コンテンツ鍵データKc
・権利書データ105
1051
SAM
1601
1052
1602
SAM
191
1604
SAM
SAM
1603
1053
1054
102
EMD
サービスセンタ
(クリアリングハウス)
KD1～KD3
カード認証局
90
ペイメントゲートウェイ
109, 166
92
利用明細書
91
決済機関
152決済
請求権データ&SIG99
103ユーザホーム
ネットワーク

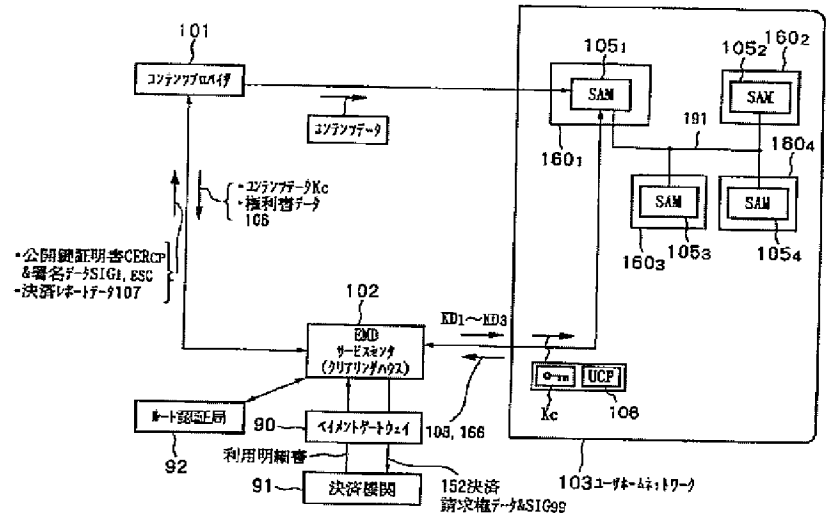
【図５６】


101
コンテンツプロバイダ
コンテンツデータ
・コンテンツ鍵データKc
・権利書データ106
1051
SAM
1601
1052
1602
SAM
191
1604
SAM
SAM
1603
1053
1054
102
KD1～KD3
KF
EMD
サービスセンタ
(クリアリングハウス)
ルート認証局
90
ペイメントゲートウェイ
108, 166
92
利用明細書
91
決済機関
152決済
請求権データ&SIG99
103ユーザホーム
ネットワーク

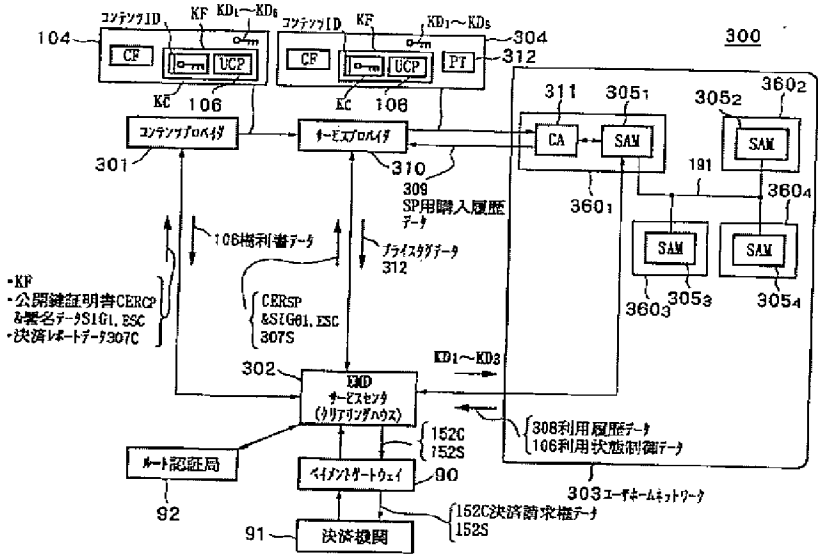
【図５７】


101
コンテンツプロバイダ
コンテンツデータ
C
Kc
UCP
106
1051
SAM
1601
1052
1602
SAM
191
1604
SAM
SAM
1603
1053
1054
・コンテンツ鍵データKc
・権利書データ106
102
KD1～KD3
EMD
サービスセンタ
(クリアリングハウス)
ルート認証局
90
ペイメントゲートウェイ
108, 166
92
利用明細書
91
決済機関
152決済
請求権データ&SIG99
103ユーザホーム
ネットワーク

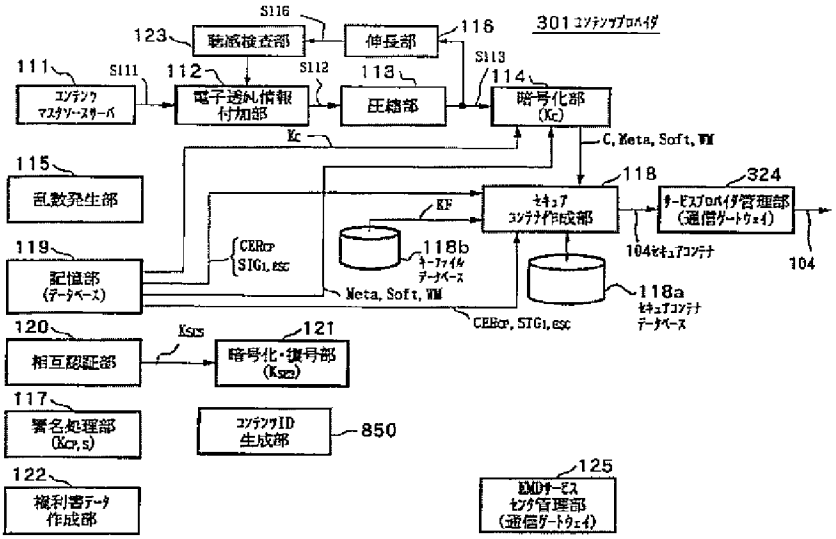
【図５８】


101
コンテンツプロバイダ
コンテンツデータ
・コンテンツデータKc
・権利書データ
105
・公開鍵証明書CERCP
&署名データSIG1, ESC
・決済レポートデータ107
102
EMD
サービスセンタ
(クリアリングハウス)
KD1～KD3
ルート認証局
92
90
ペイメントゲートウェイ
103, 166
利用明細書
91
決済機関
152決済
請求権データ&SIG99
Kc
108
1051
1052
1602
SAM
191
1601
1604
1603
1053
1054
103ユーザホームネットワーク

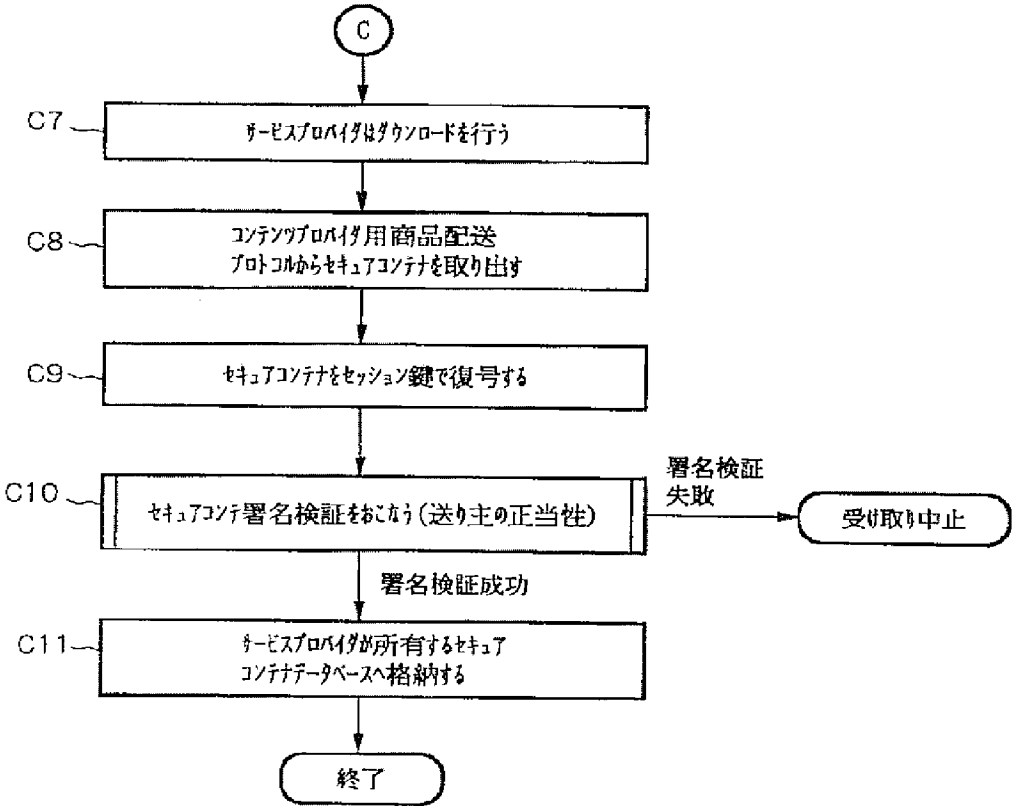
【図５９】


104
コンテンツID
KF
KD1～KDs
CF
UCP
KC
106
304
PT
312
300
311
3051
3052
3602
CA
SAM
191
3601
3604
3603
3053
3054
301
コンテンツプロバイダ
サービスプロバイダ
310
309
SP用購入履歴
データ
106権利書データ
プライスタグデータ
312
・KF
・公開鍵証明書CERCP
&署名データSIG1, ESC
・決済レポートデータ307C
CERSP
&SIG01, ESC
307S
302
EMD
サービスセンタ
(クリアリングハウス)
KD1～KD3
308利用履歴データ
106利用状態制御データ
152C
152S
ルート認証局
92
90
ペイメントゲートウェイ
303ユーザホームネットワーク
91
決済機関
152C決済請求権データ
152S

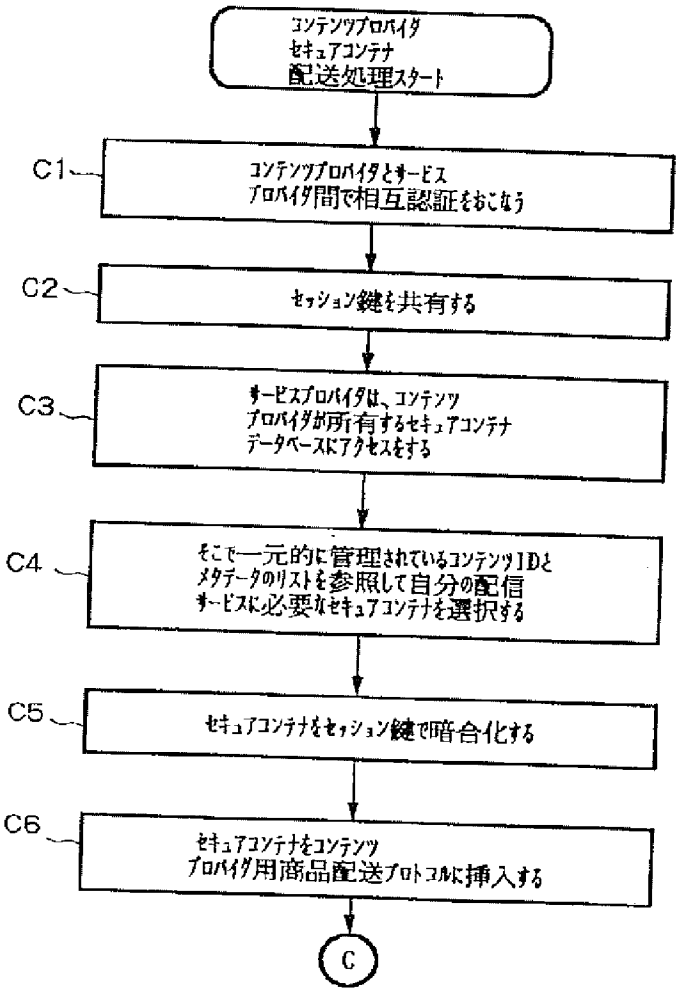
【図６０】


S116
123
著作権検査部
伸長部
116
301 コンテンツプロバイダ
111
S111
112
S112
113
S113
114
コンテンツ
マスターサーバ
電子透かし情報
付加部
圧縮部
暗号化部
(Kc)
Kc
C, Meta, Soft, WM
115
乱数発生部
118
セキュア
コンテナ作成部
324
サービスプロバイダ管理部
(通信ゲートウェイ)
KF
104セキュアコンテナ
104
119
CERcp
SIG1, esc
118b
キーファイル
データベース
記憶部
(データベース)
Meta, Soft, WM
118a
セキュアコンテナ
データベース
CERcp, SIG1, esc
120
Ksps
121
相互認証部
暗号化・復号部
(Ksps)
117
署名処理部
(Kcp, s)
コンテンツID
生成部
850
122
権利書データ
作成部
125
EMDサービス
センタ管理部
(通信ゲートウェイ)

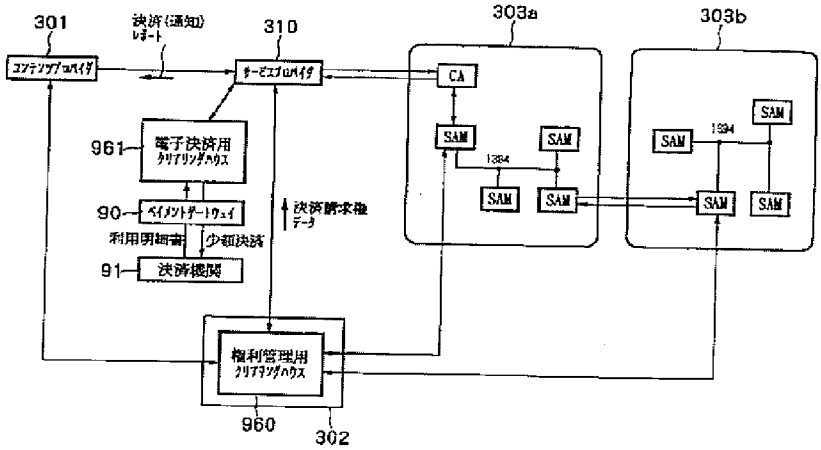
【図６２】


C
C7
サービスプロバイダはダウンロードを行う
C8
コンテンツプロバイダ用商品配送
プロトコルからセキュアコンテナを取り出す
C9
セキュアコンテナをセッション鍵で復号する
C10
セキュアコンテナ署名検証をおこなう(送り主の正当性)
署名検証
失敗
受け取り中止
署名検証成功
C11
サービスプロバイダが所有するセキュア
コンテナデータベースへ格納する
終了

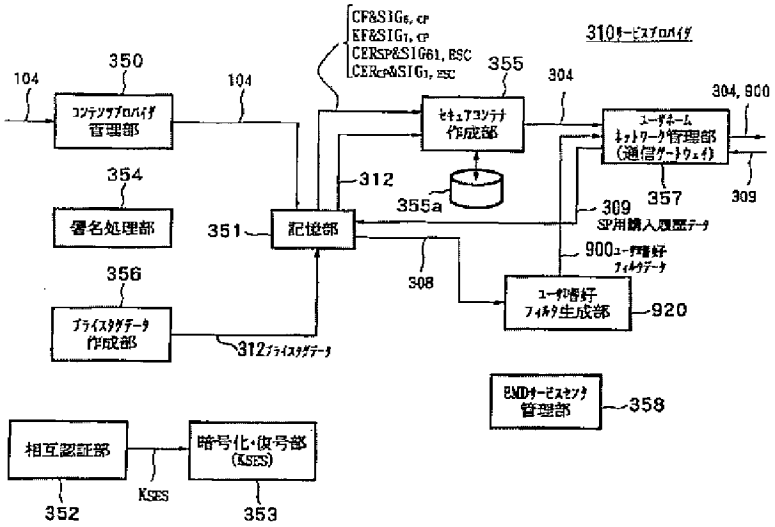
【図６１】


コンテンツプロバイダ
セキュアコンテナ
配送処理スタート
C1
コンテンツプロバイダとサービス
プロバイダ間で相互認証をおこなう
C2
セッション鍵を共有する
C3
サービスプロバイダは、コンテンツ
プロバイダが所有するセキュアコンテナ
データベースにアクセスをする
C4
そこで一元的に管理されているコンテンツIDと
メタデータのリストを参照して自分の配信
サービスに必要なセキュアコンテナを選択する
C5
セキュアコンテナをセッション鍵で暗号化する
C6
セキュアコンテナをコンテンツ
プロバイダ用商品配送プロトコルに挿入する
C

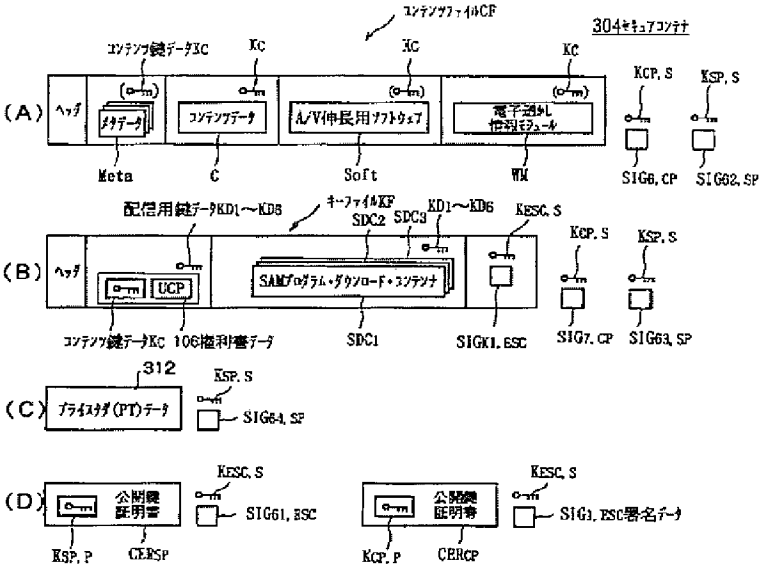
【図１０８】


301
決済(通知)
レポート
310
303a
303b
コンテンツプロバイダ
サービスプロバイダ
CA
SAM
1394
961
電子決済用
クリアリングハウス
90
ペイメントゲートウェイ
利用明細書
少額決済
91
決済機関
決済請求他
データ
権利管理用
クリアリングハウス
960
302

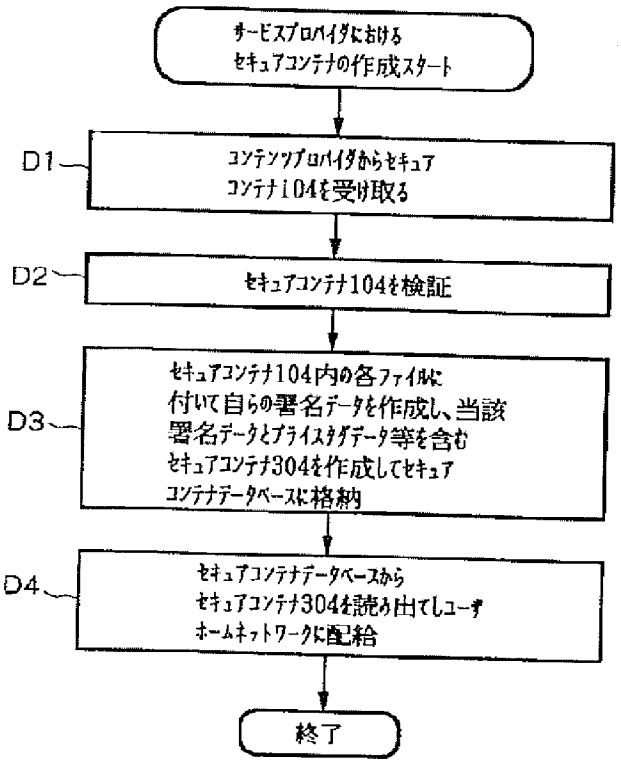
【図６３】


CF&SIG6, CP
EF&SIG1, CP
CERSP&SIG61, BSC
CERCP&SIG1, BSC
310サービスプロバイダ
350
104
104
355
304
304, 900
コンテンツプロバイダ管理部
セキュアコンテナ作成部
ユーザホームネットワーク管理部（通信ゲートウェイ）
354
312
355a
357
309
署名処理部
351
記憶部
309 SP用購入履歴データ
900ユーザ嗜好フィルタデータ
308
356
ユーザ嗜好フィルタ生成部
920
プライスタグデータ作成部
312プライスタグデータ
EMDサービスセンタ管理部
358
相互認証部
暗号化・復号部（KSES）
KSES
352
353

【図６５】


コンテンツファイルCF
304セキュアコンテナ
コンテンツ鍵データKC
KC
KC
KC
KCP, S
KSP, S
(A)
ヘッダ
メタデータ
コンテンツデータ
A/V伸長用ソフトウェア
電子透かし埋込モジュール
Meta
C
Soft
WM
SIG6, CP
SIG62, SP
配信用鍵データKD1～KD6
キーファイルKF
SDC2
SDC3
KD1～KD6
KESC, S
KCP, S
KSP, S
(B)
ヘッダ
UCP
SAMプログラム・ダウンロード・コンテンツ
コンテンツ鍵データKC
106権利書データ
SDC1
SIGK1, ESC
SIG7, CP
SIG63, SP
312
KSP, S
(C)
プライスタグ(PT)データ
SIG64, SP
KESC, S
(D)
公開鍵証明書
SIG61, ESC
KSP, P
CERSP
KESC, S
公開鍵証明書
SIG1, ESC署名データ
KCP, P
CERCP

【図６４】

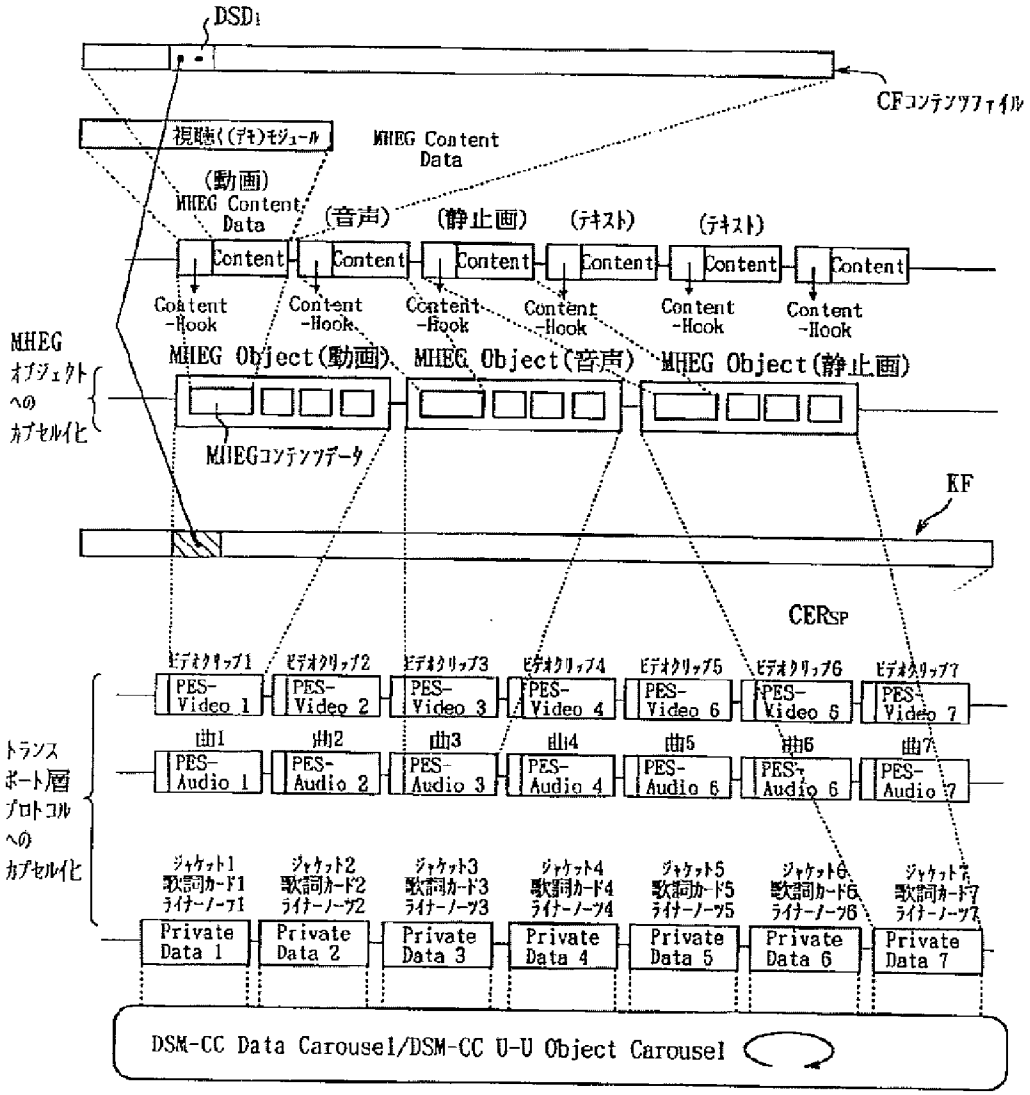


【図７７】

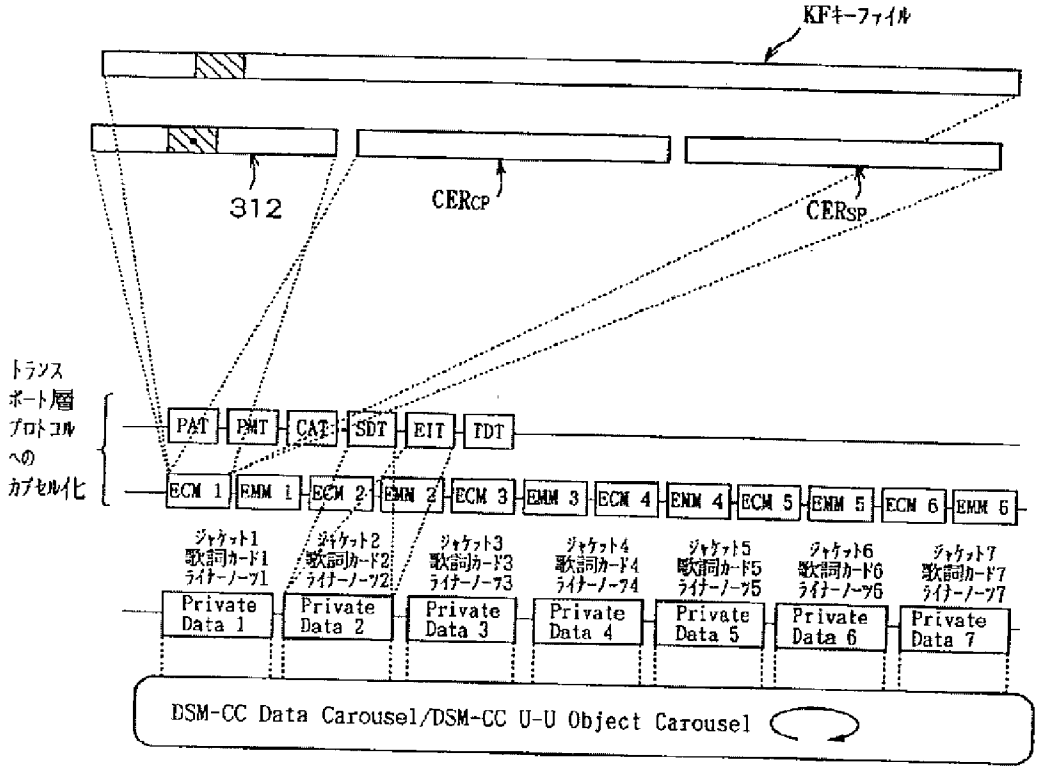
スタックメモリ200の記憶データ

コンテンツ鍵データKc
権利書データ(UCP)106
不揮発性メモリ201のロック鍵データK_{Loc}
コンテンツプロバイダ301の公開鍵証明書データCER_{CP}
サービスプロバイダ301の公開鍵証明書データCER_{SP}
利用制御情状態データ(UCS)166
SAMプログラム・ダウンロード・コンテナSD_1～SDC_3
プライスタグデータ312

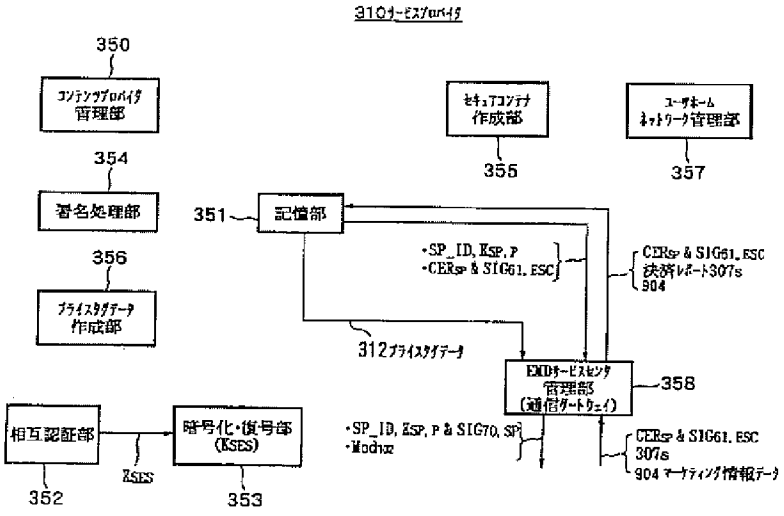
【図６６】


DSD1
CFコンテンツファイル
視聴(デモ)モジュール
MHEG Content Data
(動画)
MHEG Content Data
(音声)
(静止画)
(テキスト)
(テキスト)
Content
Content-Hook
MHEG オブジェクトへのカプセル化
MHEG Object(動画)
MHEG Object(音声)
MHEG Object(静止画)
MHEGコンテンツデータ
KF
CERSP
ビデオクリップ1
PES-Video 1
曲1
PES-Audio 1
ジャケット1 歌詞カード1 ライナーノーツ1
Private Data 1
トランスポート層プロトコルへのカプセル化
DSM-CC Data Carousel/DSM-CC U-U Object Carousel

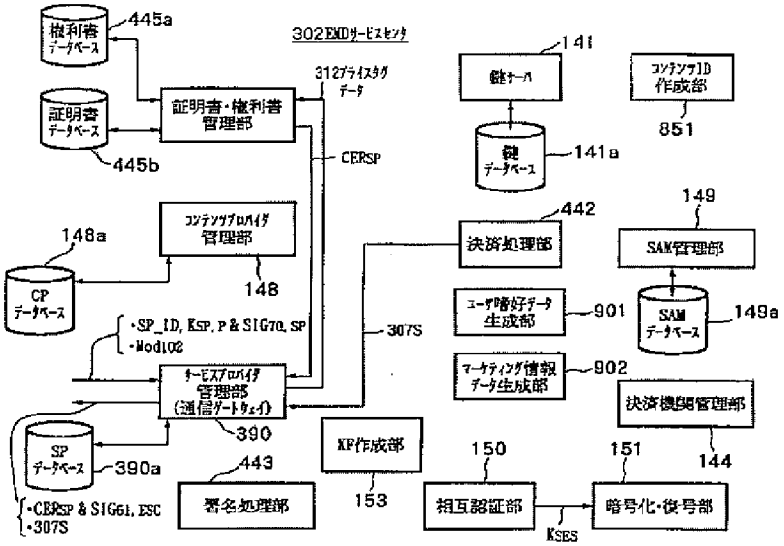
【図６７】


KFキーファイル
312
CERCP
CERSP
トランスポート層プロトコルへのカプセル化
PAT
PMT
CAT
SDT
EIT
TDT
ECM 1
EMM 1
ECM 2
EMM 2
ECM 3
EMM 3
ECM 4
EMM 4
ECM 5
EMM 5
ECM 6
EMM 6
Private Data 1
Private Data 2
Private Data 3
Private Data 4
Private Data 5
Private Data 6
Private Data 7
DSM-CC Data Carousel/DSM-CC U-U Object Carousel

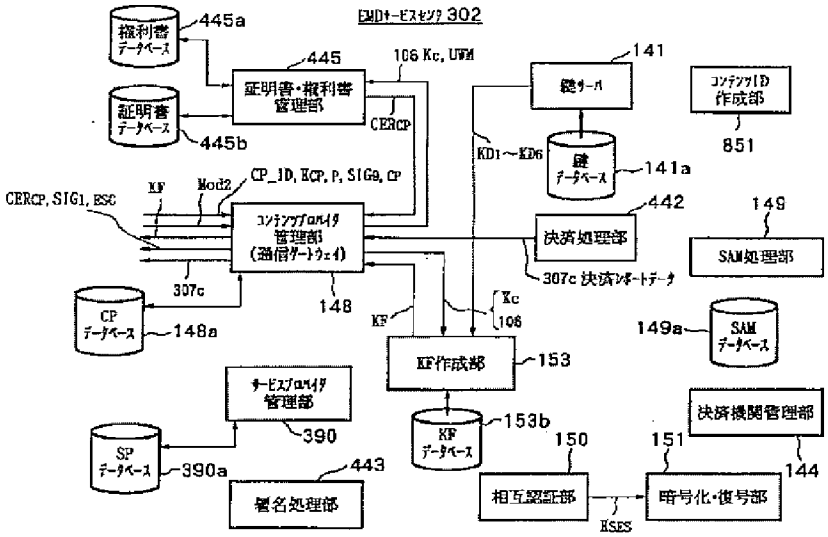
【図６８】


350
354
356
351
記憶部
355
357
358
352
353
312
相互認証部
暗号化・復号部
(KSES)
KSES
CERSP & SIG61, ESC
307s
904

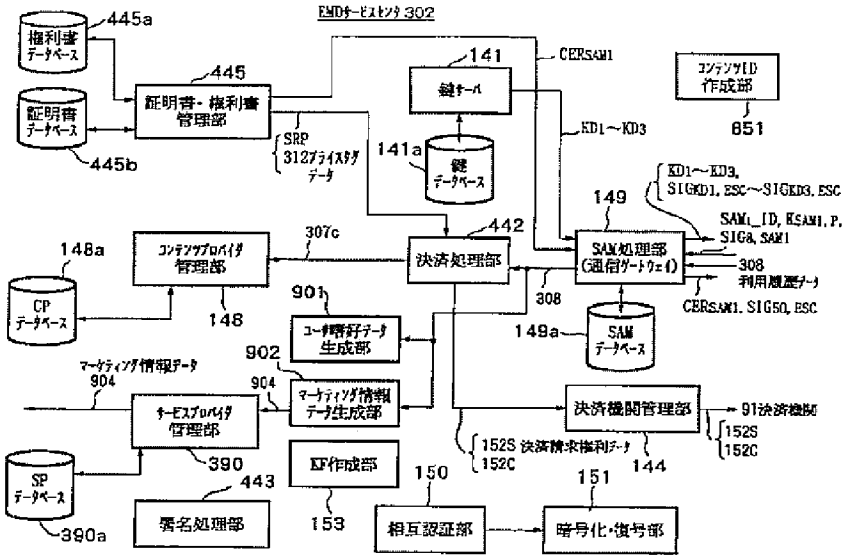
【図７０】


権利書データベース
445a
302 EMDサービスセンタ
312 プライスタグデータ
証明書データベース
445b
証明書・権利書管理部
CERSP
141
鍵サーバ
コンテンツID作成部
851
鍵データベース
141a
コンテンツプロバイダ管理部
148
148a
CPデータベース
442
決済処理部
149
SAM管理部
・SP_ID, KSP, P & SIG70, SP
・Mod102
307S
ユーザ嗜好データ生成部
901
SAMデータベース
149a
マーケティング情報データ生成部
902
サービスプロバイダ管理部（通信ゲートウェイ）
390
決済機関管理部
144
SPデータベース
390a
KF作成部
153
150
151
443
署名処理部
相互認証部
暗号化・復号部
KSES
・CERSP & SIG61, ESC
・307S

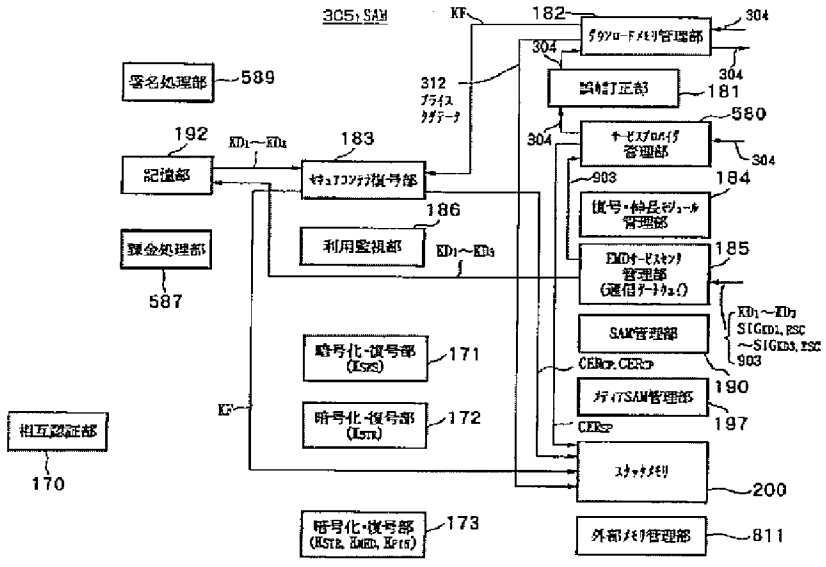
【図７１】


権利書データベース
445a
EMDサービスセンタ 302
445
106 Kc, UWM
証明書・権利書管理部
CERCP
証明書データベース
445b
141
鍵サーバ
コンテンツID作成部
851
KD1～KD6
鍵データベース
141a
CERCP, SIG1, ESC
KF
Mod2
CP_ID, KCP, P, SIG9, CP
コンテンツプロバイダ管理部（通信ゲートウェイ）
442
決済処理部
149
SAM処理部
307c 決済レポートデータ
307c
148
CPデータベース
148a
KF
Kc
106
149a
SAMデータベース
KF作成部
153
サービスプロバイダ管理部
390
決済機関管理部
KFデータベース
153b
150
151
144
SPデータベース
390a
443
署名処理部
相互認証部
暗号化・復号部
KSES

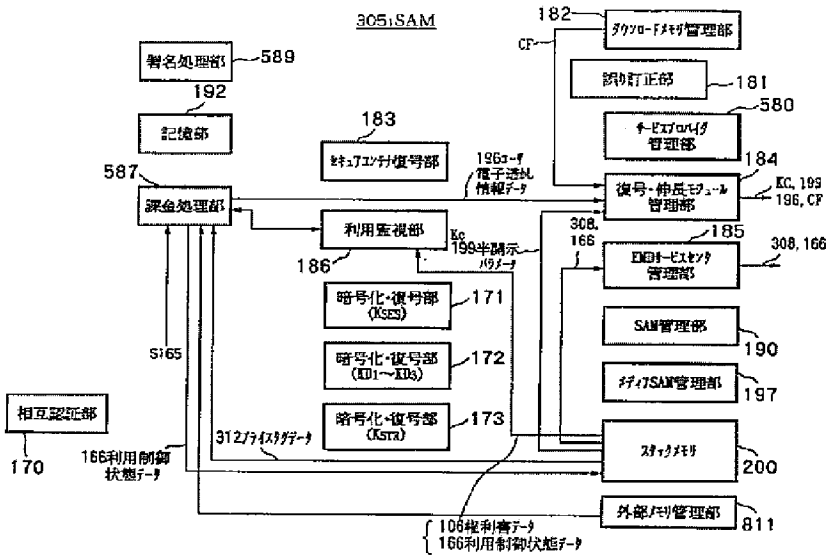
【図７２】


EMDサービスセンタ 302
権利書データベース
445a
証明書データベース
445b
証明書・権利書管理部
445
SRP 312プライスタグデータ
鍵チーバ
141
CERSAM1
KD1～KD3
鍵データベース
141a
コンテンツID作成部
651
KD1～KD3, SIGKD1, ESC～SIGKD3, ESC
SAM1_ID, RSAM1, P, SIG8, SAM1
149
SAM処理部（通信ゲートウェイ）
308
利用履歴データ
CERSAM1, SIG50, ESC
SAM データベース
149a
決済処理部
442
308
コンテンツプロバイダ管理部
307c
148a
CP データベース
148
901
ユーザ嗜好データ生成部
902
マーケティング情報データ
904
サービスプロバイダ管理部
390
マーケティング情報データ生成部
904
決済機関管理部
91決済機関
152S 決済請求権利データ
152C
144
KF作成部
153
150
151
SP データベース
390a
署名処理部
443
相互認証部
暗号化・復号部

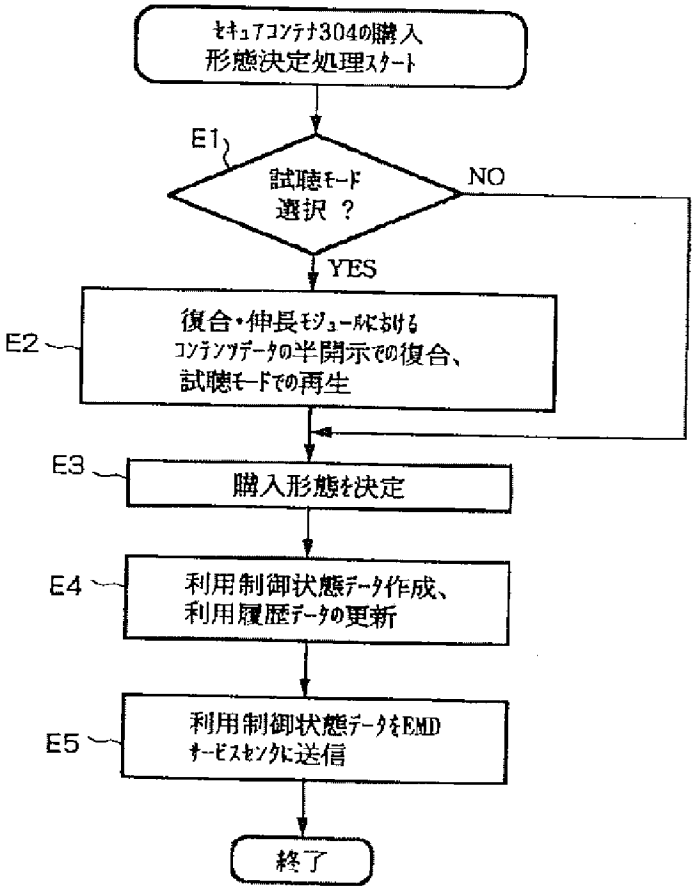
【図７６】


305, SAM
KF
182
ダウンロードメモリ管理部
304
署名処理部
589
312 プライスタグデータ
時計訂正部
181
192
記憶部
KD1～KD3
183
セキュアコンテンツ復号部
サービスプロバイダ管理部
580
903
184
復号・伸長モジュール管理部
186
利用監視部
KD1～KD3
課金処理部
587
EMDサービスセンタ管理部（通信データウェイ）
185
SAM管理部
KD1～KD3 SIGKD1, ESC ～SIGKD3, ESC
903
CERCP, CERCP
暗号化・復号部 (KSES)
171
メディアSAM管理部
190
197
KF
暗号化・復号部 (KSTR)
172
CERCP
相互認証部
170
スナックメモリ
200
暗号化・復号部 (KSTR, KMID, KFIX)
173
外部メモリ管理部
811

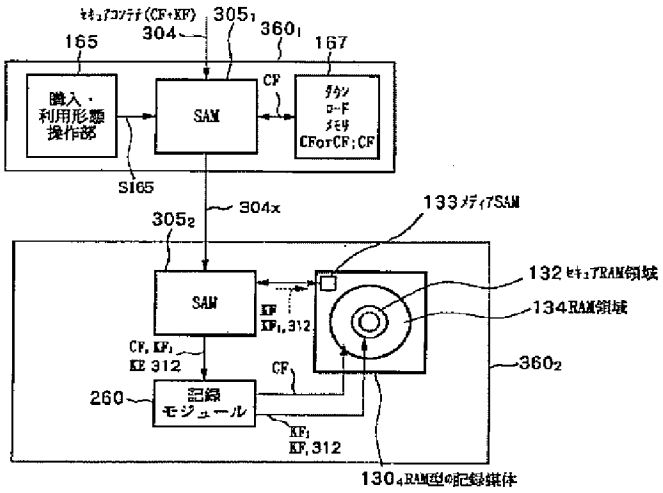
【図７８】


305:SAM
署名処理部
589
192
記憶部
587
課金処理部
183
セキュアコンテナ復号部
利用監視部
186
暗号化・復号部 (KSES)
171
暗号化・復号部 (KD1～KDs)
172
暗号化・復号部 (KSTR)
173
S165
相互認証部
170
166利用制御状態データ
312プライスタグデータ
196コード電子透かし情報データ
Kc 199半開示パラメータ
182
ダウンロードメモリ管理部
CF
誤り訂正部
181
580
サービスプロバイダ管理部
184
復号・伸長モジュール管理部
KC, 193
196, CF
308, 166
185
EMDサービスセンタ管理部
308, 166
SAM管理部
190
メディアSAM管理部
197
スタックメモリ
200
外部メモリ管理部
811
106視聴履歴データ
166利用制御状態データ

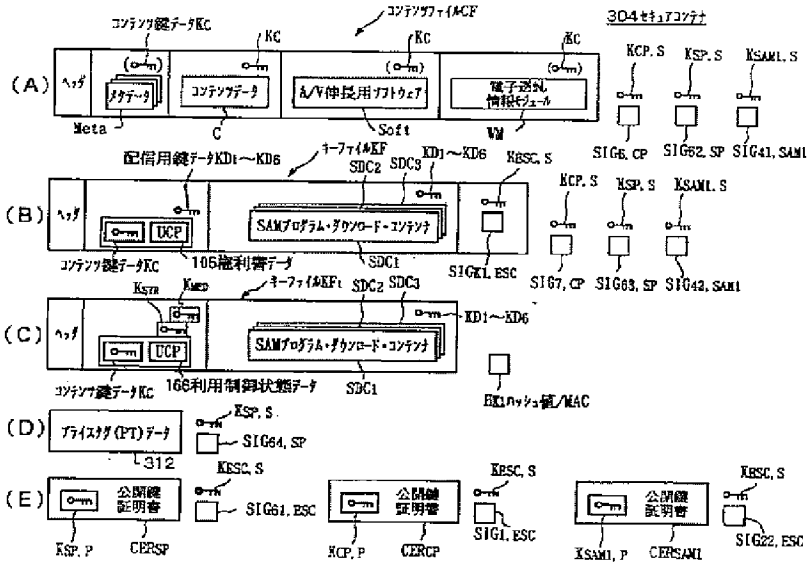
【図７９】


セキュアコンテナ304の購入形態決定処理スタート
E1
試聴モード選択 ？
NO
YES
E2
復合・伸長モジュールにおけるコンテンツデータの半開示での復合、試聴モードでの再生
E3
購入形態を決定
E4
利用制御状態データ作成、利用履歴データの更新
E5
利用制御状態データをEMDサービスセンタに送信
終了

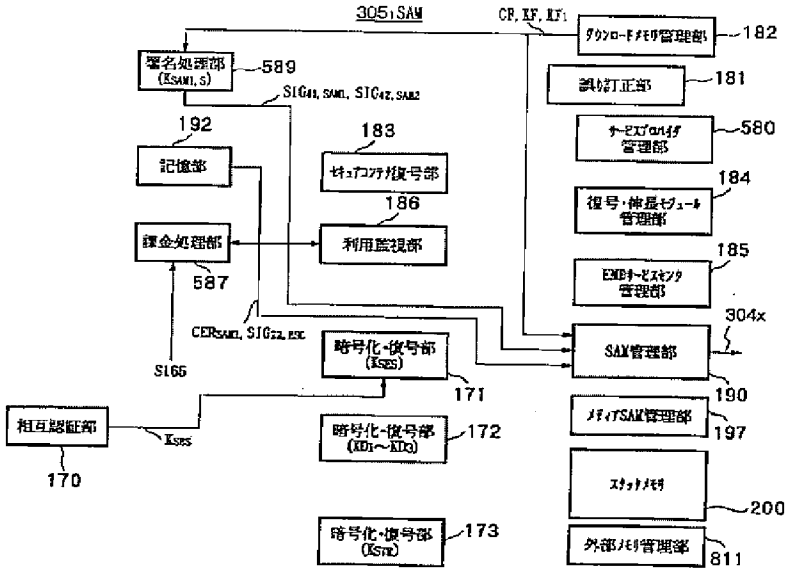
【図８０】


165
304
167
CF
SAM
SI65
304x
SAM
CF
260
記録
モジュール
132
134RAM領域
360₂
130 RAM型の記録媒体

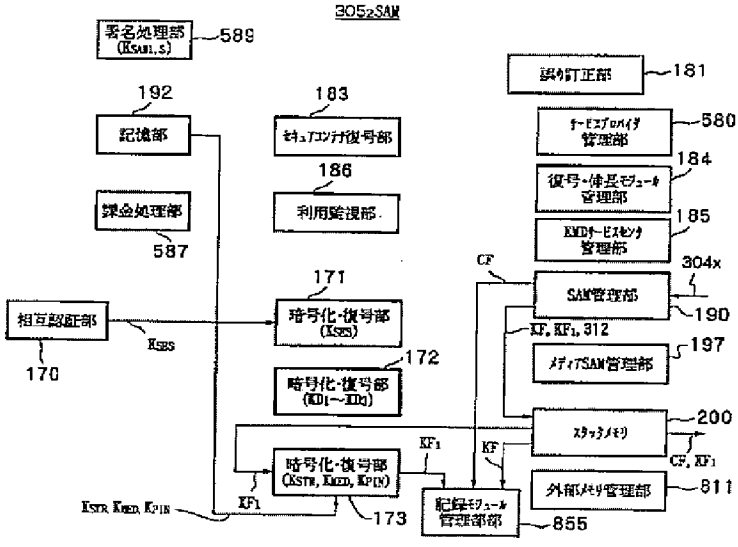
【図８１】


(A)
Meta
C
Soft
VM
(B)
UCP
SAMプログラム・ダウンロード・コンテンツ
(C)
UCP
SAMプログラム・ダウンロード・コンテンツ
(D)
(E)
公開鍵証明書
公開鍵証明書
公開鍵証明書

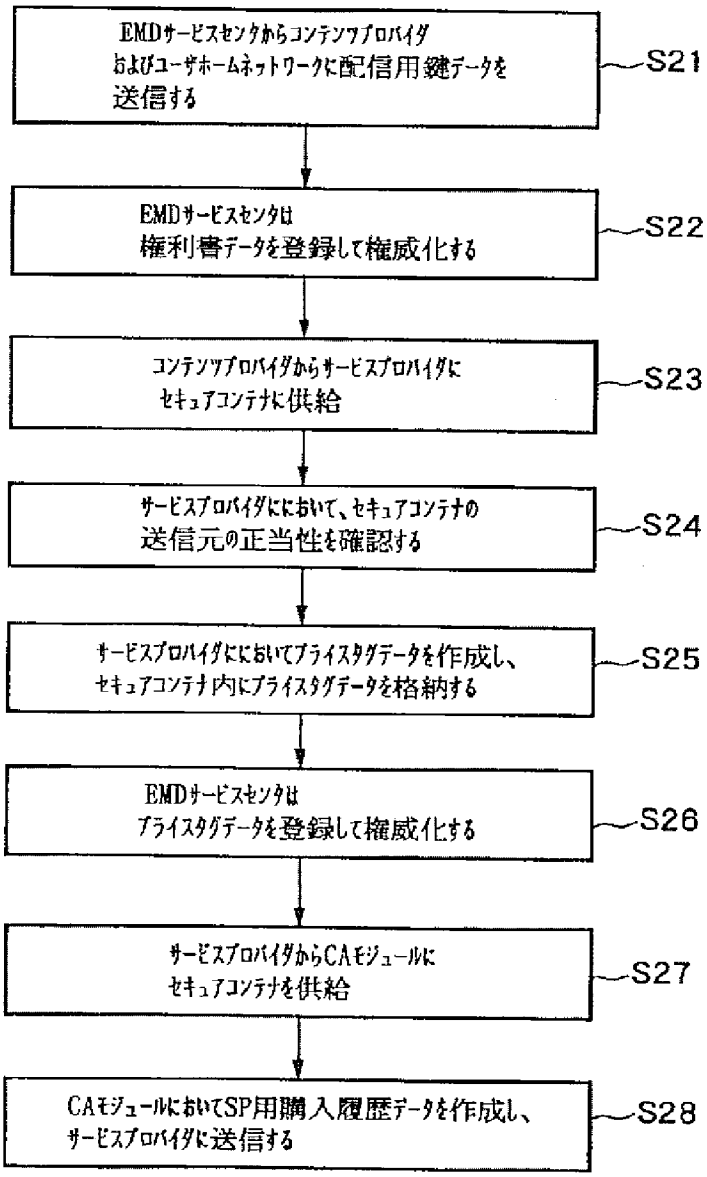
【図８２】


305₁SAM
CF, KF, KF₁
ダウンロードメモリ管理部
182
署名処理部
(KSAM1, S)
589
誤り訂正部
181
SIG41, SAM1, SIG42, SAM2
192
記憶部
183
セキュアコンテナ復号部
サービスプロバイダ管理部
580
186
184
復号・伸長モジュール管理部
課金処理部
利用監視部
587
185
EMDサービスセンタ管理部
304x
CERSAM1, SIG22, ESC
暗号化・復号部
(KSES)
SAM管理部
S165
171
190
メディアSAM管理部
197
相互認証部
KSES
暗号化・復号部
(KD1～KDq)
172
170
スタックメモリ
200
暗号化・復号部
(KSTR)
173
外部メモリ管理部
811

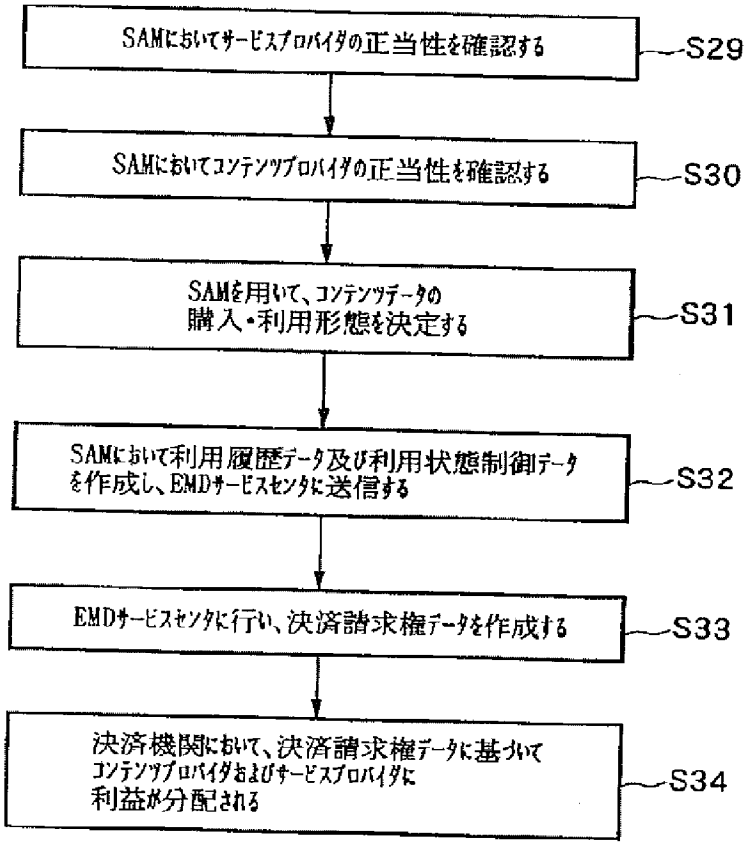
【図８３】


305₂SAM
署名処理部
(KSAM1, S)
589
誤り訂正部
181
192
記憶部
183
セキュアコンテナ復号部
サービスプロバイダ管理部
580
186
184
復号・伸長モジュール管理部
課金処理部
利用監視部
587
185
EMDサービスセンタ管理部
CF
304x
SAM管理部
171
190
KF, KF1, 312
相互認証部
KSES
暗号化・復号部
(KSES)
197
メディアSAM管理部
172
暗号化・復号部
(KD1～KDq)
170
200
スタックメモリ
KF1
KF
暗号化・復号部
(KSTR, KMED, KP1N)
CF, KF1
外部メモリ管理部
811
KF1
KSTR, KMED, KP1N
173
記録モジュール管理部
855

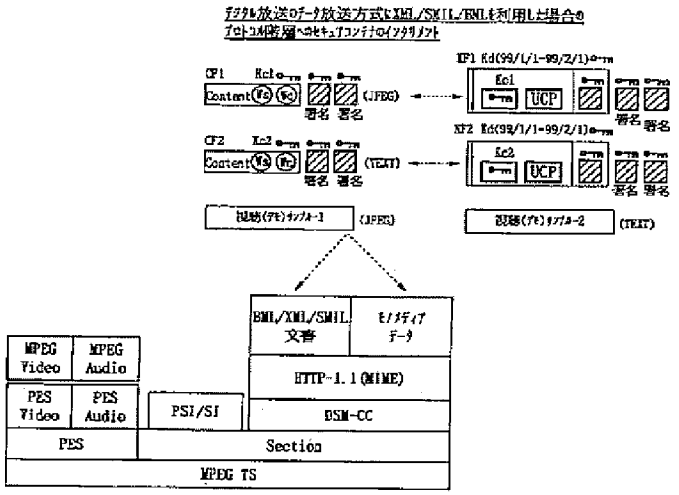
【図８４】


EMDサービスセンタからコンテンツプロバイダおよびユーザホームネットワークに配信用鍵データを送信する
S21
EMDサービスセンタは権利書データを登録して権威化する
S22
コンテンツプロバイダからサービスプロバイダにセキュアコンテナに供給
S23
サービスプロバイダにおいて、セキュアコンテナの送信元の正当性を確認する
S24
サービスプロバイダにおいてプライスタグデータを作成し、セキュアコンテナ内にプライスタグデータを格納する
S25
EMDサービスセンタはプライスタグデータを登録して権威化する
S26
サービスプロバイダからCAモジュールにセキュアコンテナを供給
S27
CAモジュールにおいてSP用購入履歴データを作成し、サービスプロバイダに送信する
S28

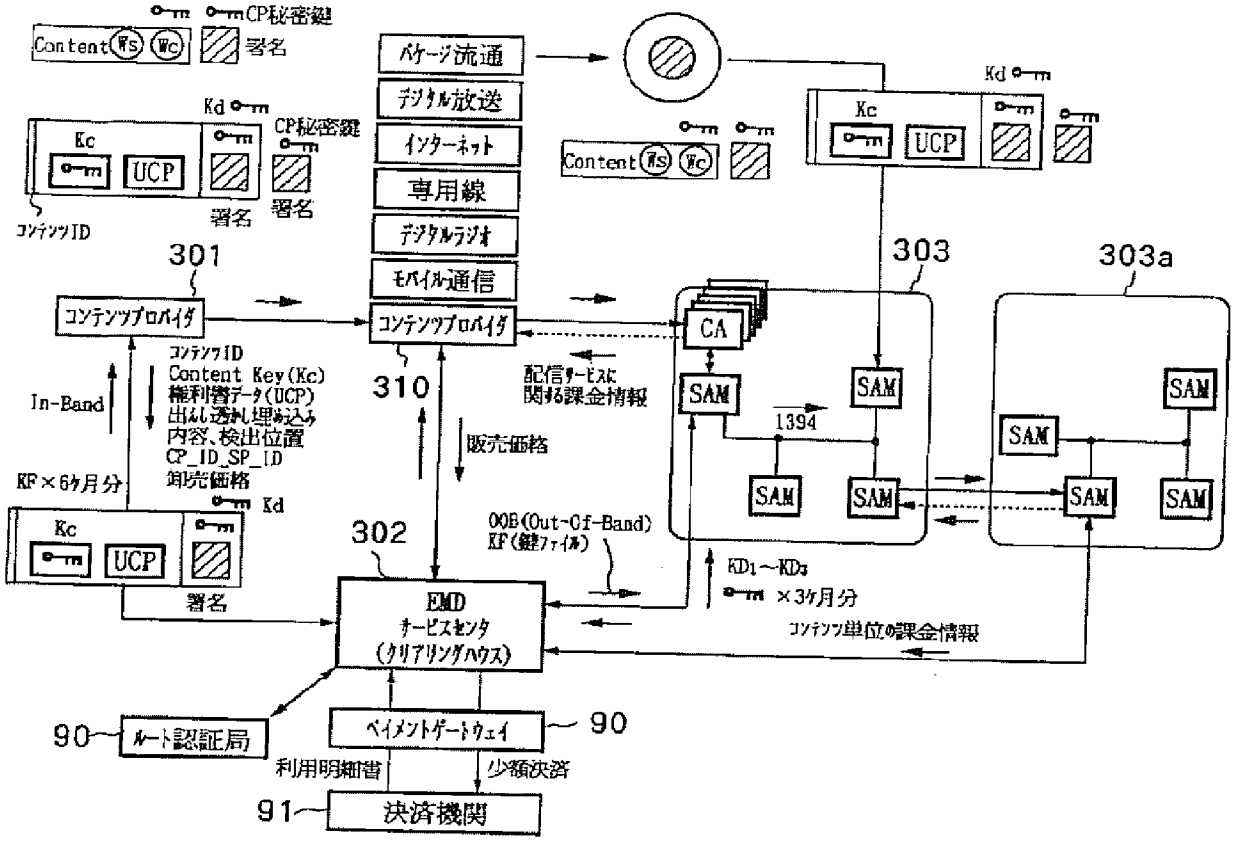
【図８５】


SAMにおいてサービスプロバイダの正当性を確認する
S29
SAMにおいてコンテンツプロバイダの正当性を確認する
S30
SAMを用いて、コンテンツデータの
購入・利用形態を決定する
S31
SAMにおいて利用履歴データ及び利用状態制御データ
を作成し、EMDサービスセンタに送信する
S32
EMDサービスセンタに行い、決済請求権データを作成する
S33
決済機関において、決済請求権データに基づいて
コンテンツプロバイダおよびサービスプロバイダに
利益が分配される
S34

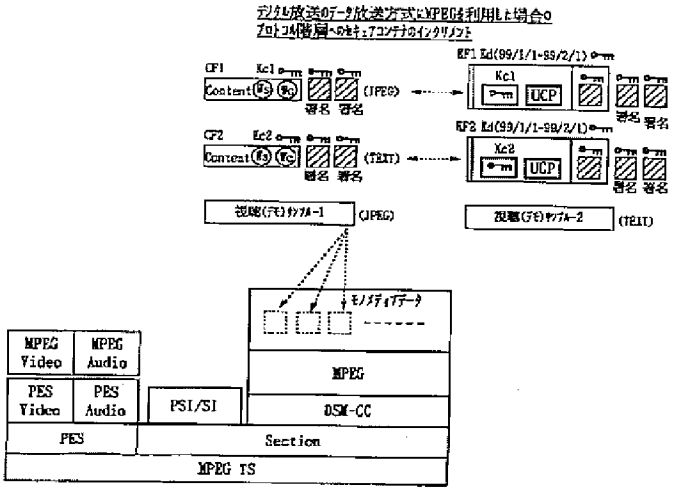
【図９２】


MPEG Video
MPEG Audio
PES Video
PES Audio
PSI/SI
PES
Section
MPEG TS
HTTP-1.1(MIME)
DSM-CC
UCP
(JPEG)
(TEXT)

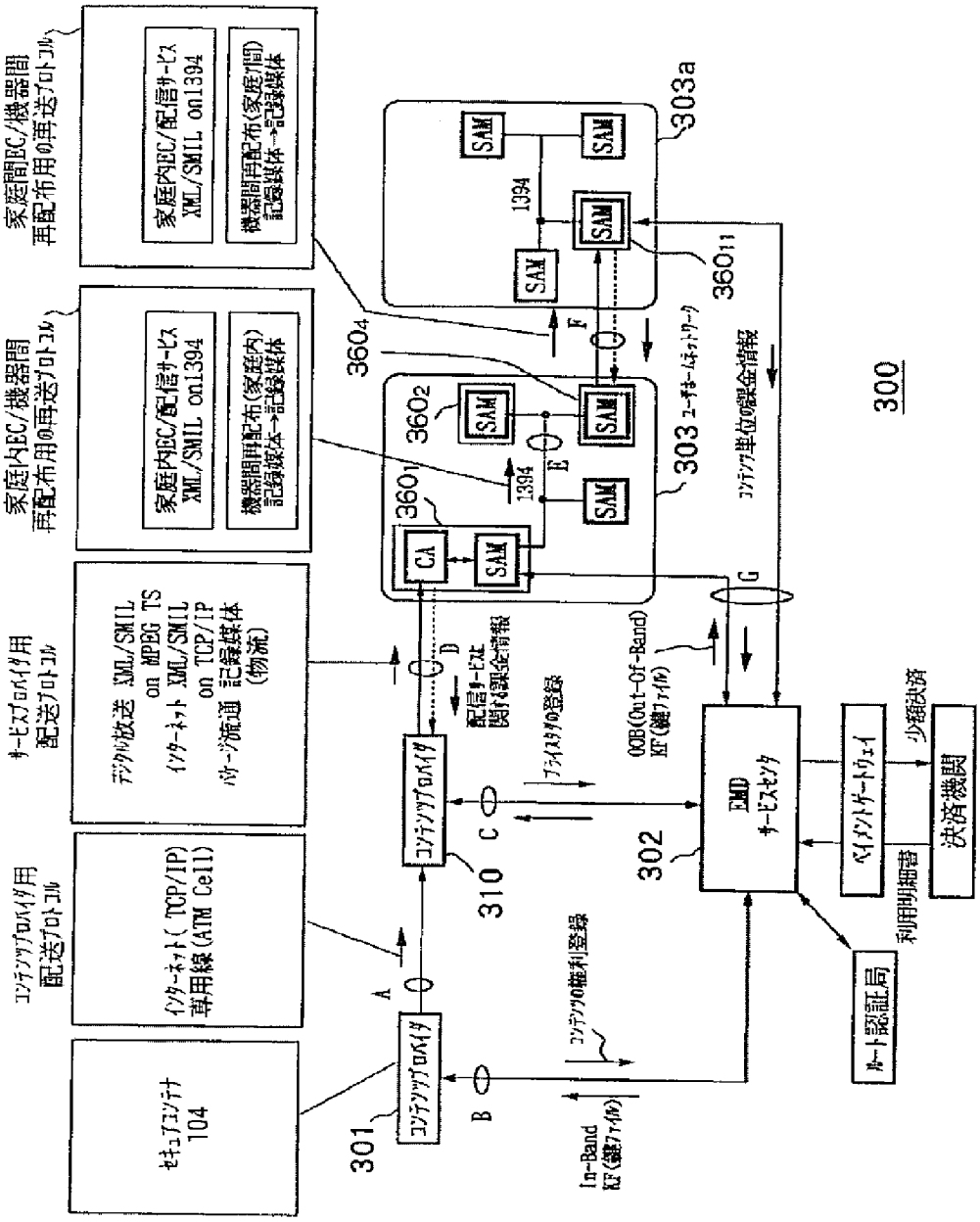
【図８６】


CP秘密鍵
Content
Ws
Wc
署名
Kd
Kc
UCP
CP秘密鍵
署名
署名
コンテンツID
パケージ流通
デジタル放送
インターネット
専用線
デジタルラジオ
モバイル通信
301
コンテンツプロバイダ
コンテンツプロバイダ
303
303a
CA
SAM
SAM
SAM
SAM
SAM
SAM
SAM
SAM
1394
コンテンツID
Content Key(Kc)
権利書データ(UCP)
出力透かし埋め込み
内容、検出位置
CP_ID,SP_ID
卸売価格
In-Band
KF×6ヶ月分
310
販売価格
配信サービスに
関する課金情報
302
OOB(Out-Of-Band)
KF(鍵ファイル)
KD1～KDn
×3ヶ月分
コンテンツ単位の課金情報
EMD
サービスセンタ
(クリアリングハウス)
90
ルート認証局
ペイメントゲートウェイ
90
利用明細書
少額決済
91
決済機関

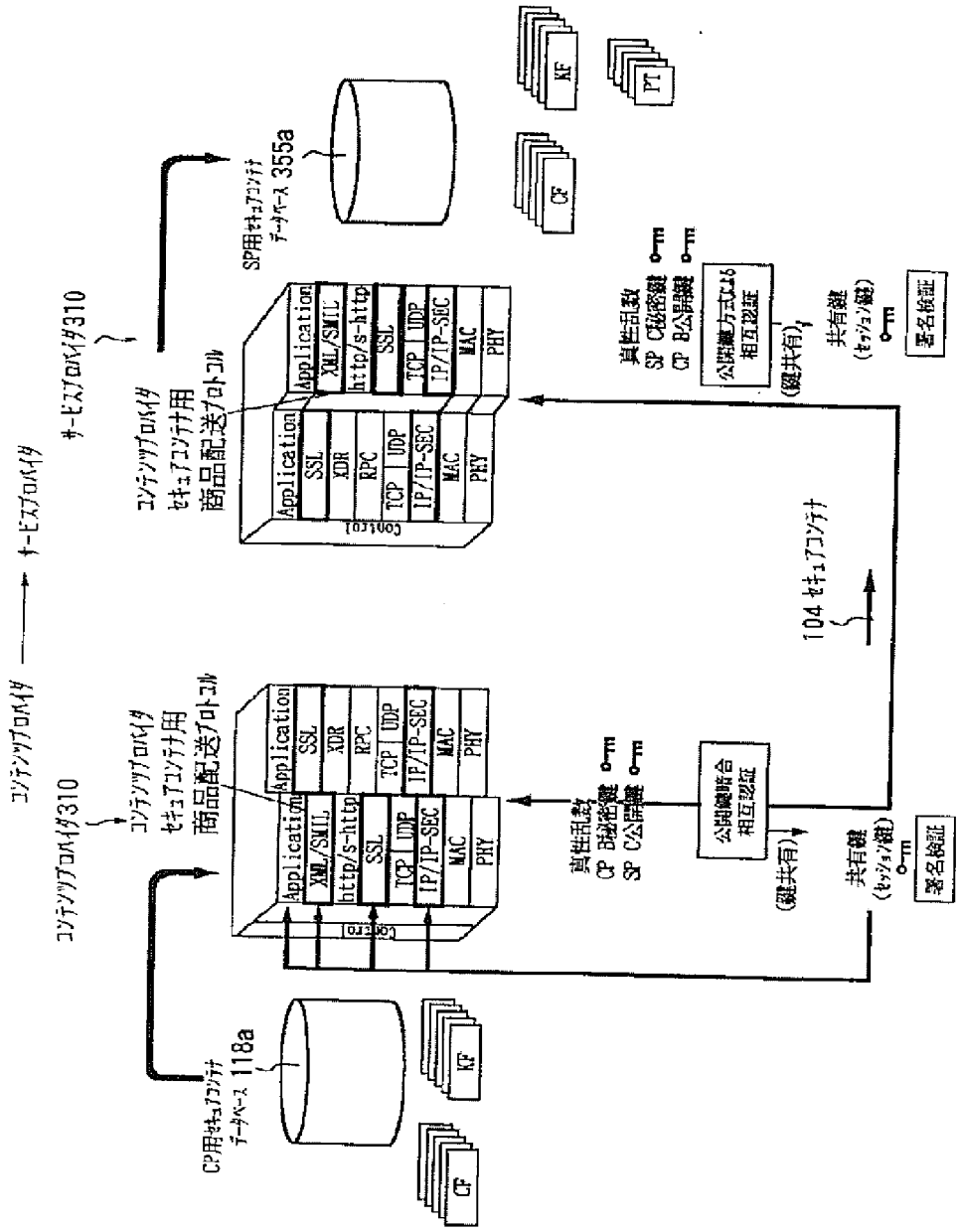
【図９３】


MPEG Video
MPEG Audio
PES Video
PES Audio
PSI/SI
PES
Section
MPEG TS
MPEG
DSM-CC

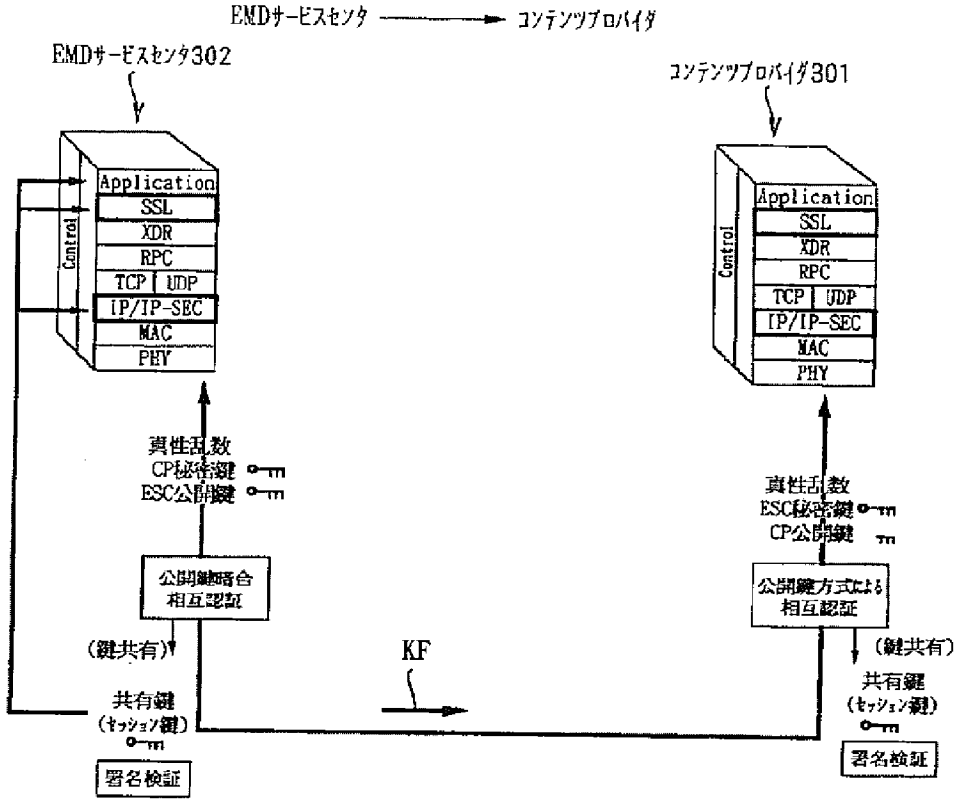
【図８７】


家庭間EC/機器間
再配布用の再送プロトコル
家庭内EC/配信サービス
XML/SMIL on1394
機器間再配布(家庭間)
記録媒体→記録媒体
家庭内EC/機器間
再配布用の再送プロトコル
家庭内EC/配信サービス
XML/SMIL on1394
機器間再配布(家庭内)
記録媒体→記録媒体
サービスプロバイダ用
配送プロトコル
デジタル放送 XML/SMIL
on MPEG TS
インターネット XML/SMIL
on TCP/IP
パッケージ流通 記録媒体
(物流)
コンテンツプロバイダ用
配送プロトコル
インターネット(TCP/IP)
専用線(ATM Cell)
セキュアコンテナ
104
301
コンテンツプロバイダ
310
コンテンツプロバイダ
302
EMD
サービスセンタ
303
ユーザホームネットワーク
303a
SAM
CA
1394
360₁
360₂
360₃
360₄
360₁₁
300
コンテンツ単位課金情報
配信サービス
関係課金情報
ライセンスの登録
OOB(Out-Of-Band)
KF(鍵ファイル)
In-Band
KF(鍵ファイル)
コンテンツの権利登録
ペイントゲートウェイ
少額決済
決済機関
利用明細書
ルート認証局
A
B
C
D
E
F
G

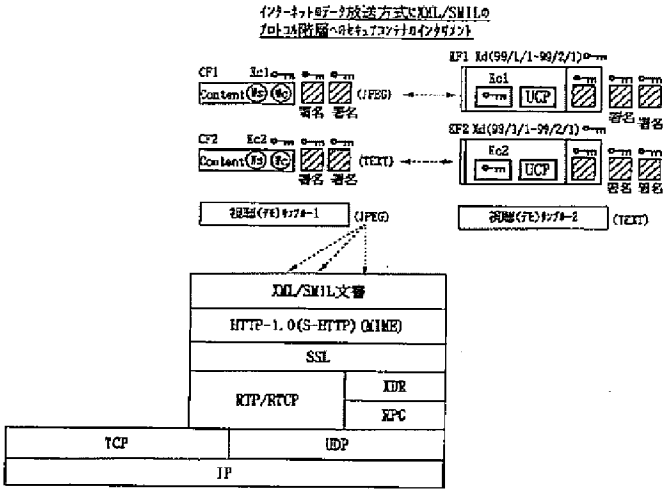
【図８８】


コンテンツプロバイダ
サービスプロバイダ
コンテンツプロバイダ310
サービスプロバイダ310
コンテンツプロバイダ
セキュアコンテナ用
商品配送プロトコル
CP用セキュアコンテナ
データベース 118a
SP用セキュアコンテナ
データベース 355a
Application
XML/SMIL
http/s-http
SSL
XDR
RPC
TCP
UDP
IP/IP-SEC
MAC
PHY
KF
CF
PT
CP 秘密鍵
SP C公開鍵
公開鍵方式による
相互認証
(鍵共有)
共有鍵
(セッション鍵)
署名検証
104 セキュアコンテナ

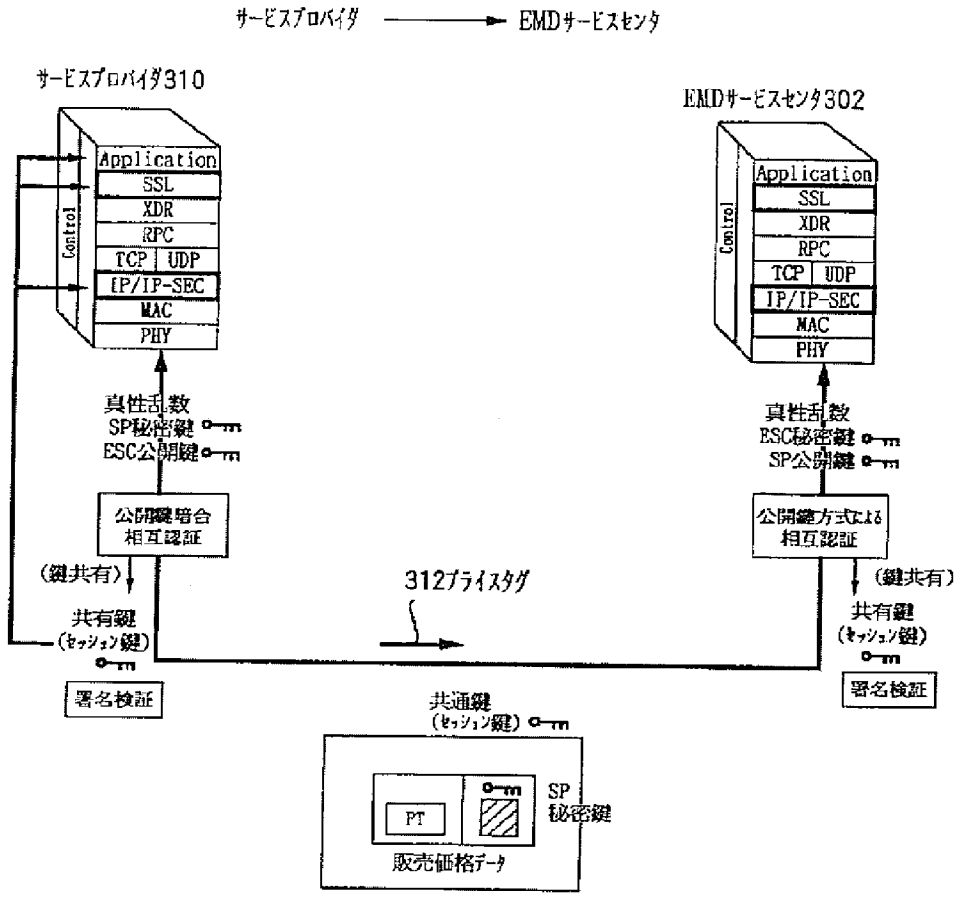
【図８９】


EMDサービスセンタ
コンテンツプロバイダ
EMDサービスセンタ302
コンテンツプロバイダ301
Application
SSL
XDR
RPC
TCP
UDP
IP/IP-SEC
MAC
PHY
Control
真性乱数
CP秘密鍵
ESC公開鍵
公開鍵暗号相互認証
(鍵共有)
共有鍵
(セッション鍵)
署名検証
KF
真性乱数
ESC秘密鍵
CP公開鍵
公開鍵方式による相互認証
(鍵共有)
共有鍵
(セッション鍵)
署名検証

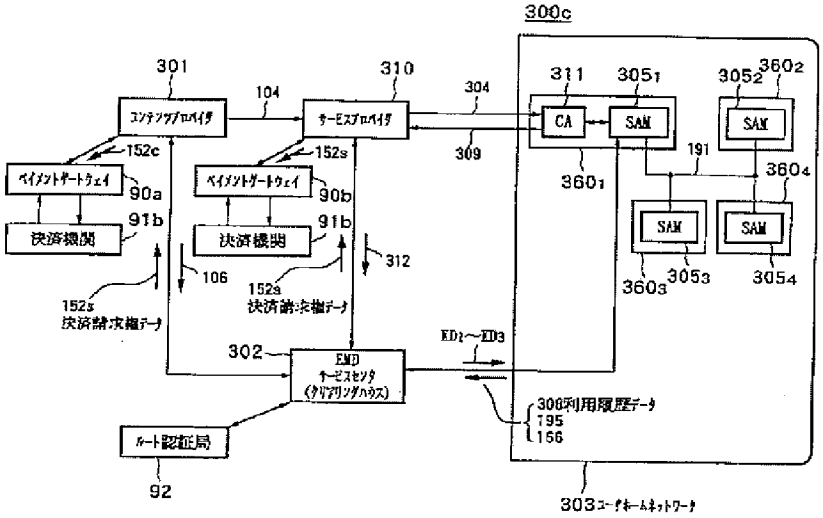
【図９４】


XML/SMIL文書
HTTP-1.0(S-HTTP) (MIME)
SSL
RTP/RTCP
XDR
XPC
TCP
UDP
IP

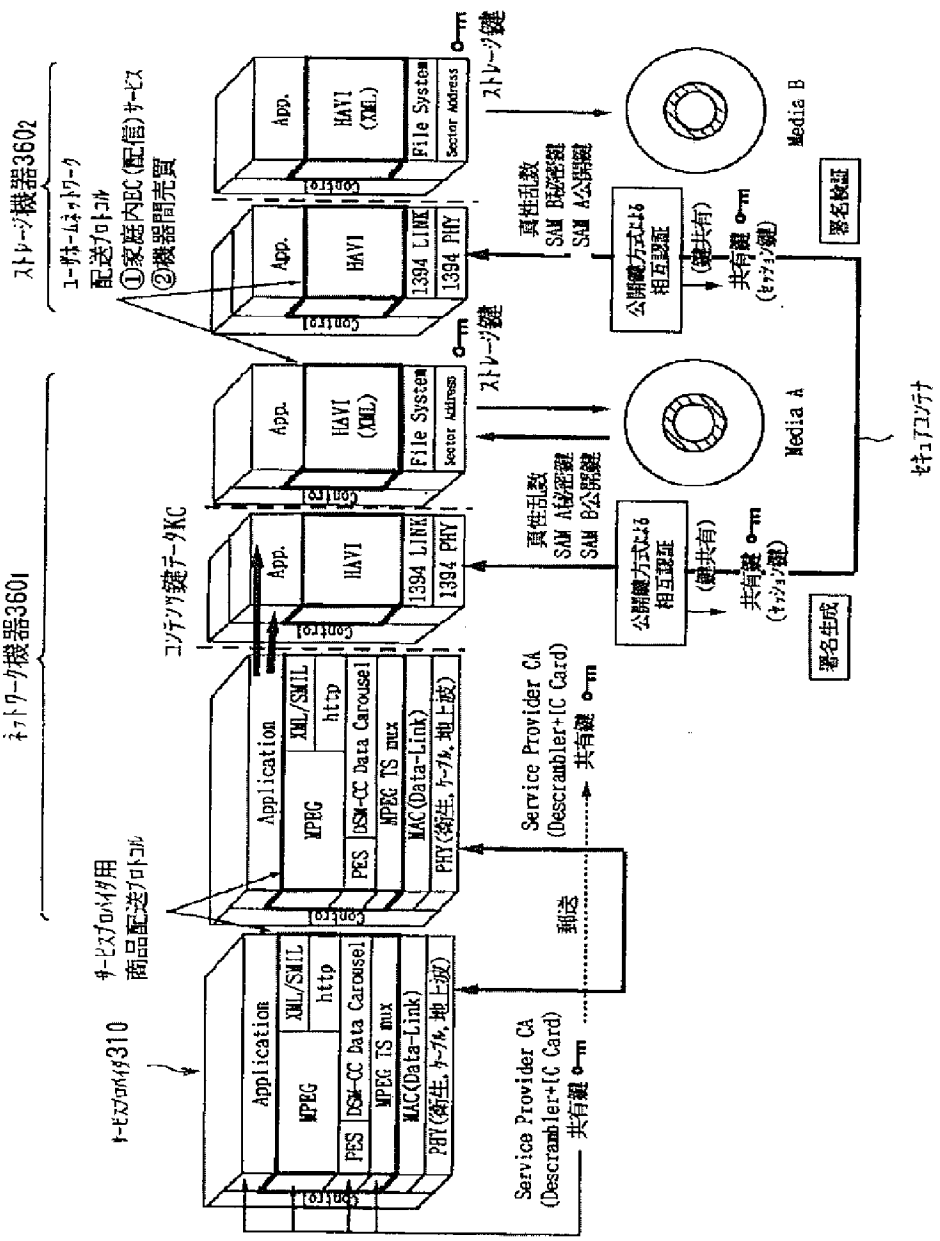
【図９０】


サービスプロバイダ
EMDサービスセンタ
サービスプロバイダ310
EMDサービスセンタ302
Application
SSL
XDR
RPC
TCP
UDP
IP/IP-SEC
MAC
PHY
Control
真性乱数
SP秘密鍵
ESC公開鍵
公開鍵暗合
相互認証
(鍵共有)
共有鍵
(セッション鍵)
署名検証
真性乱数
ESC秘密鍵
SP公開鍵
公開鍵方式による
相互認証
(鍵共有)
共有鍵
(セッション鍵)
署名検証
312プライスタグ
共通鍵
(セッション鍵)
PT
SP
秘密鍵
販売価格データ

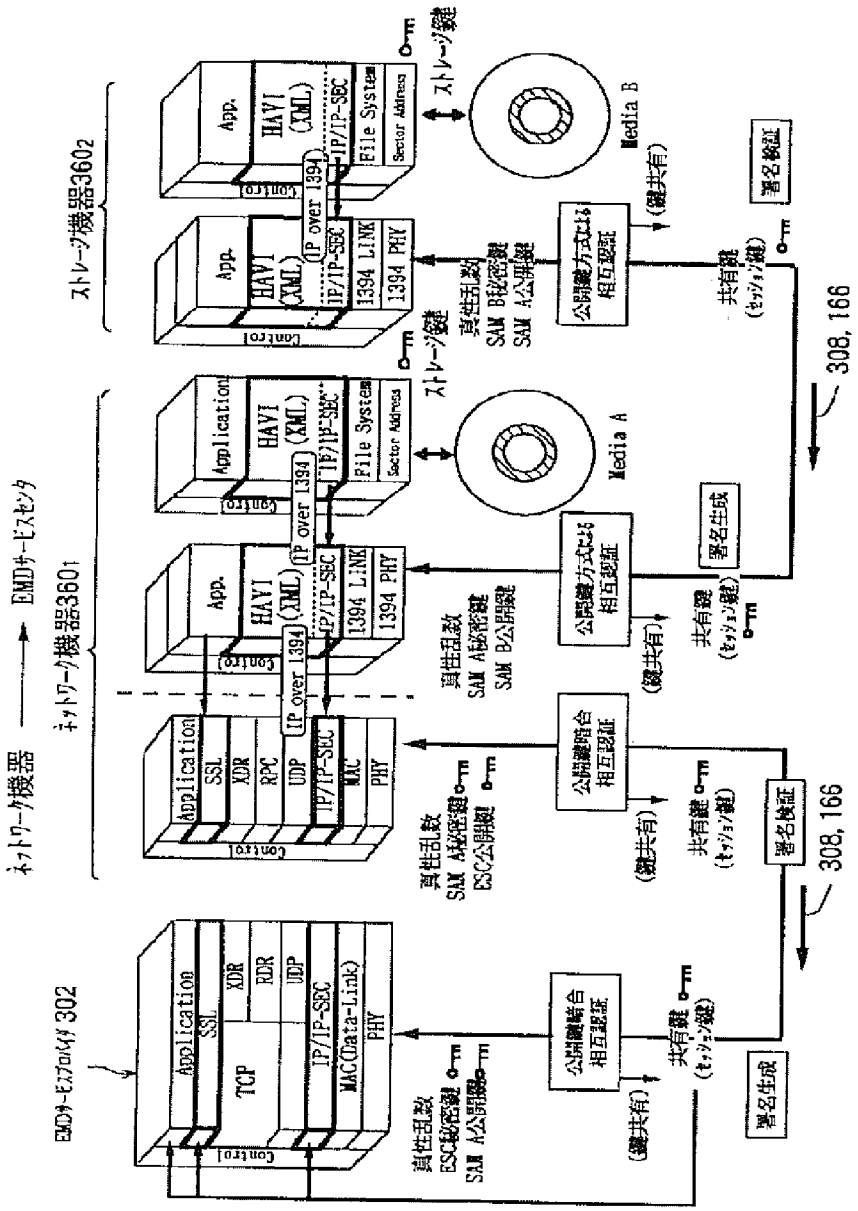
【図９９】


300c
301
310
104
304
311
305₁
3052
360₂
CA
SAM
309
191
360₁
360₄
152c
152s
90a
90b
91b
決済機関
106
312
360₃
305₃
305₄
152s
決済請求権データ
302
EMD
サービスセンタ
(クリアリングハウス)
ED₂～ED₃
300利用履歴データ
195
156
ルート認証局
92
303ユーザホームネットワーク

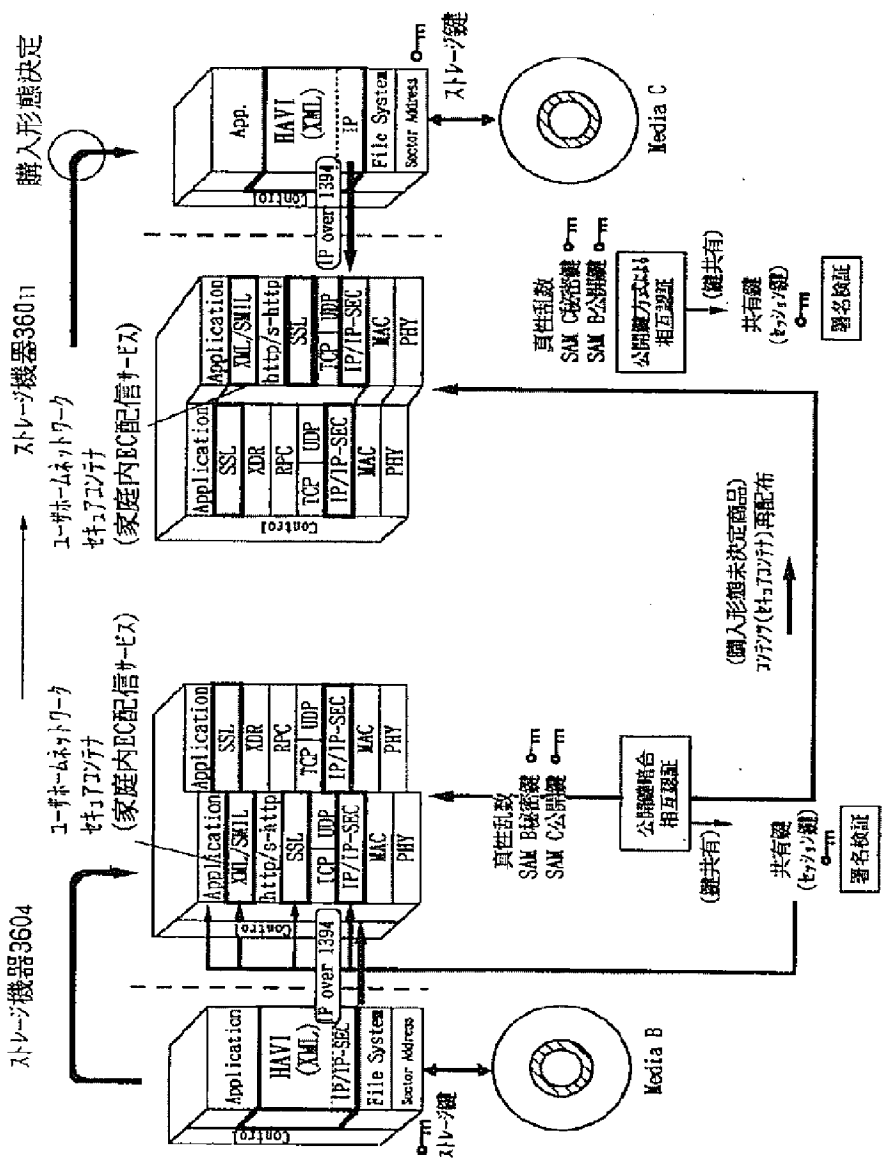
【図９１】


ネットワーク機器3601
ストレージ機器3602
ユーザネットワーク
配送プロトコル
①家庭内EC(配信)サービス
②機器間売買
サービスプロバイダ用
商品配送プロトコル
サービスプロバイダ310
コンテンツ鍵データMC
ストレージ鍵
App.
HAVi (XML)
File System
Sector Address
HAVi
1394 LINK
1394 PHY
Application
XML/SMIL
http
MPEG
PES
DSM-CC Data Carousel
MPEG TS mux
MAC(Data-Link)
PHY(変生, ケーブル, 地上波)
Service Provider CA
(Descrambler+IC Card)
共有鍵
郵送
真性乱数
SAM B秘密鍵
SAM A公開鍵
公開鍵方式による
相互認証
(鍵共有)
共有鍵
(セッション鍵)
署名生成
署名検証
Media A
Media B
セキュアコンテナ

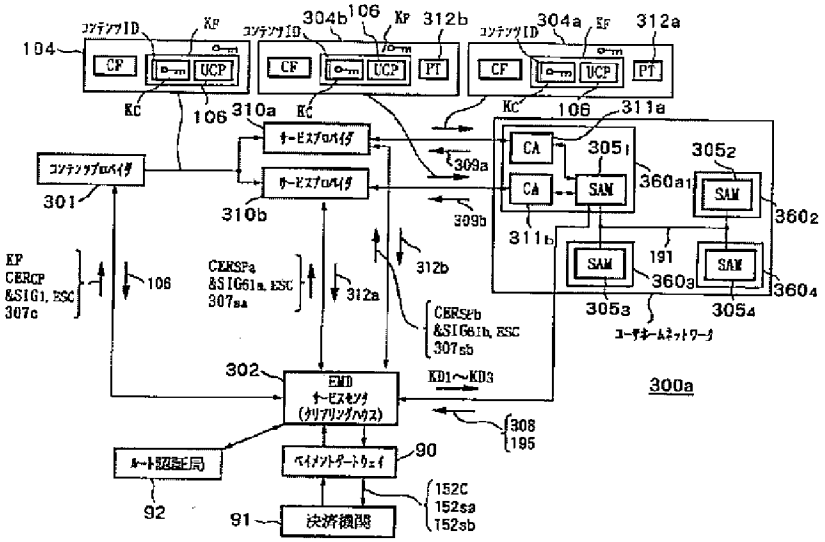
【図９５】


ネットワーク機器
EMDサービスセンタ
ネットワーク機器360₁
ストレージ機器360₂
EMDサービス302
Application
SSL
XDR
RPC
UDP
TCP
IP/IP-SEC
MAC(Data-Link)
PHY
Control
HAVI (XML)
App.
IP over 1394
1394 LINK
1394 PHY
File System
Sector Address
Media A
Media B
ストレージ鍵
真性乱数
SAM A秘密鍵
SAM A公開鍵
SAM B秘密鍵
SAM B公開鍵
ESC秘密鍵
ESC公開鍵
公開鍵方式による相互認証
(鍵共有)
共有鍵
(セッション鍵)
署名生成
署名検証
308, 166

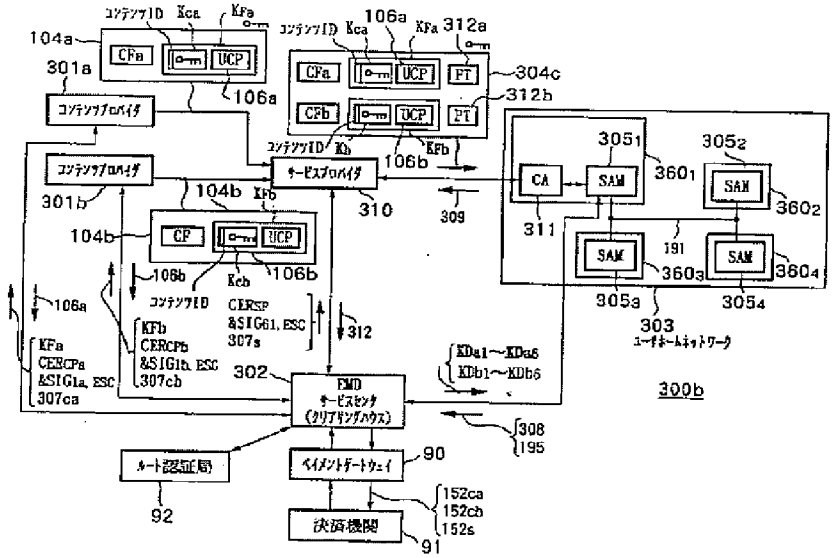
【図９６】


購入形態決定
ストレージ機器3604
ストレージ機器3601
ユーザホームネットワーク
セキュアコンテナ
(家庭内EC配信サービス)
ユーザホームネットワーク
セキュアコンテナ
(家庭内EC配信サービス)
Application
HAVI (XML)
IP/IP-SEC
File System
Sector Address
Control
IP over 1394
App.
IP
ストレージ鍵
Media B
Media C
Application
XML/SMIL
http/s-http
SSL
TCP
UDP
IP/IP-SEC
MAC
PHY
XDR
RPC
真性乱数
SAM B秘密鍵
SAM C公開鍵
公開鍵暗号相互認証
(鍵共有)
共有鍵
(セッション鍵)
署名検証
(購入形態未決定商品)
コンテンツ(セキュアコンテナ)再配布

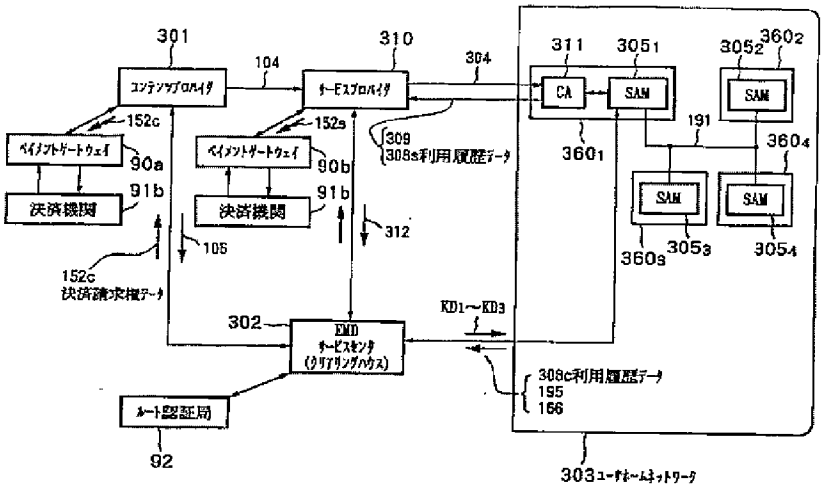
【図９７】


104
CF
UCP
PT
KF
KC
106
304b
304a
312b
312a
310a
310b
311a
311b
301
309a
309b
CA
SAM
305₁
305₂
305₃
305₄
360a₁
360₂
360₃
360₄
191
312b
312a
KF
CERCP
&SIG1, ESC
307c
CERSPa
&SIG61a, ESC
307sa
CERSPb
&SIG61b, ESC
307sb
302
EMD
KD1～KD3
300a
308
195
90
91
92
152C
152sa
152sb
決済機関

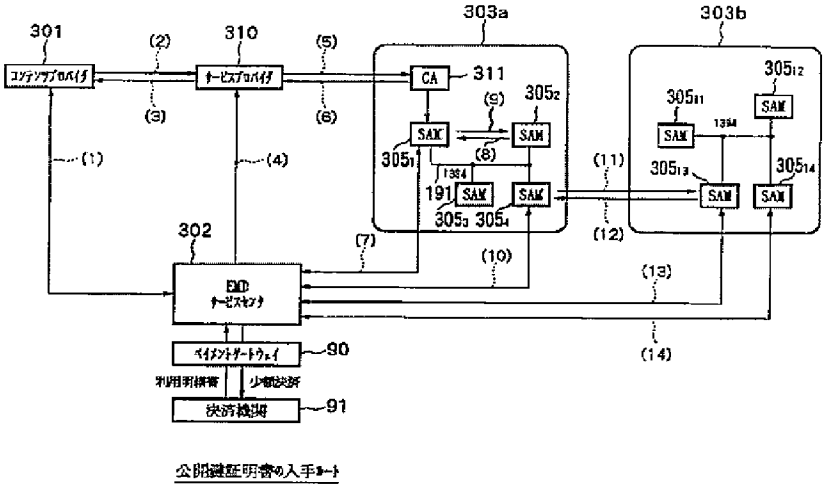
【図９８】


104a
104b
301a
301b
106a
106b
106
310
309
311
312a
312b
304c
CFa
CFb
UCP
PT
KFa
KFb
Kca
Kcb
KCb
CERSP
&SIG61, ESC
307s
KFa
CERCPa
&SIG1a, ESC
307ca
KFb
CERCPb
&SIG1b, ESC
307cb
312
302
EMD
KDa1～KDa6
KDb1～KDb6
300b
308
195
90
91
92
152ca
152cb
152s
決済機関
303

【図１００】

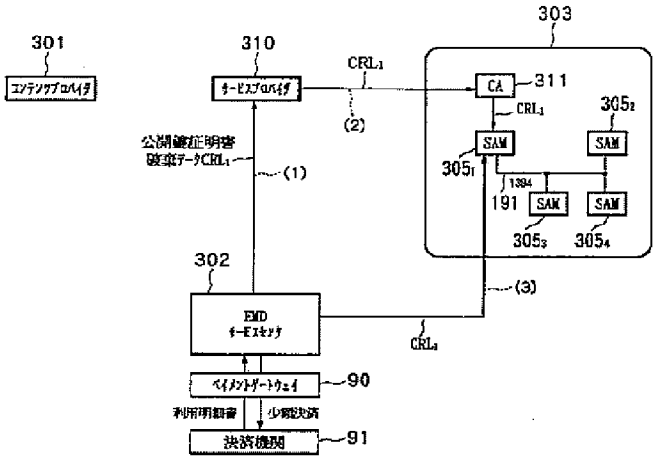


【図１０１】



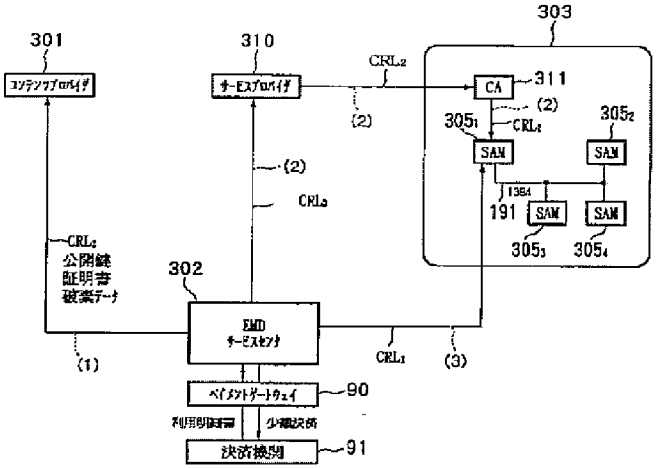
公開鍵証明書の入手ルート

【図１０２】



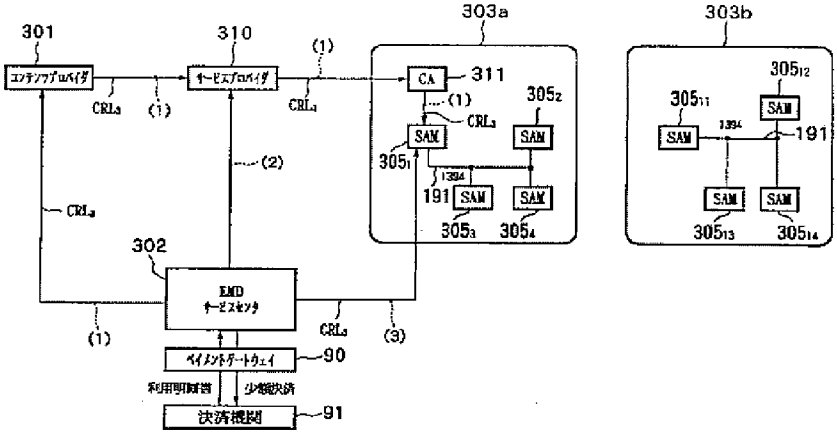
CERcpを無効にする場合

【図１０３】



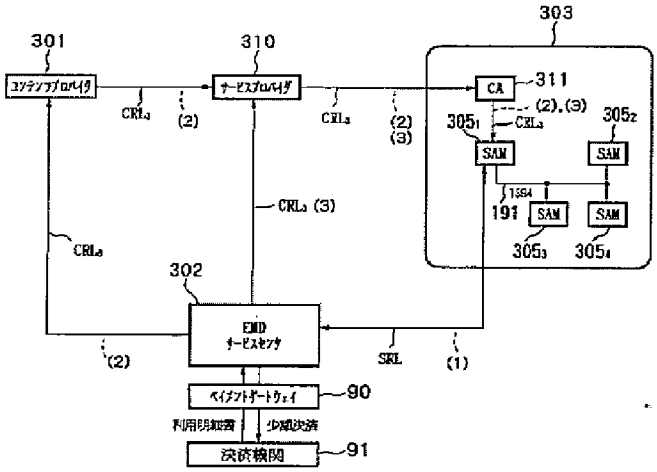
CERspを無効にする場合

【図１０４】

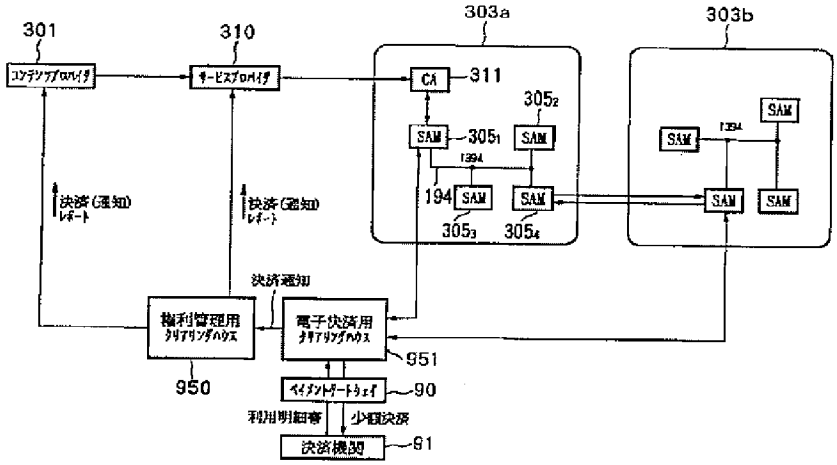


CERSAM2を無効にする場合

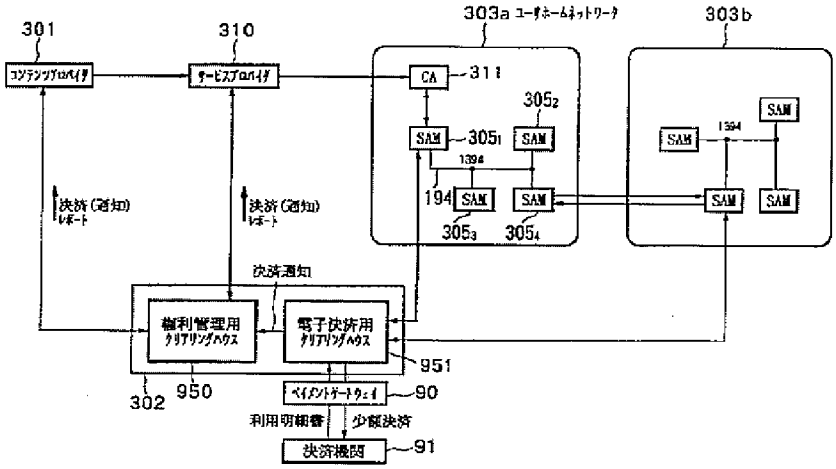
【図１０５】



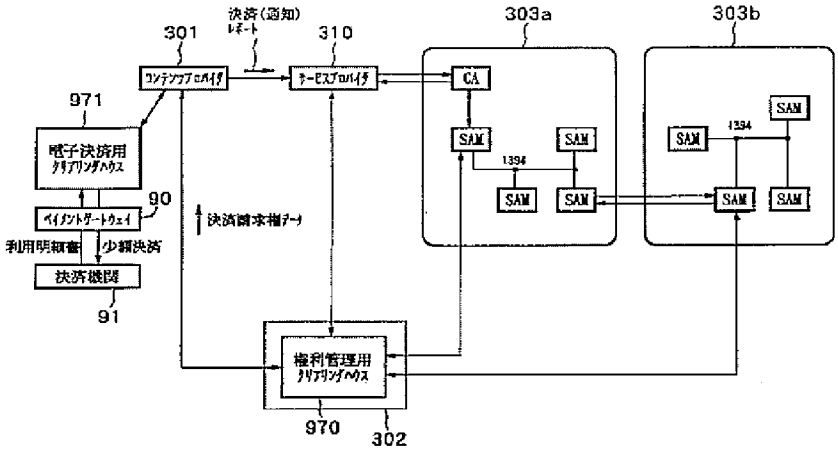
【図１０６】


301
310
303a
303b
CA
311
SAM
305₁
305₂
305₃
305₄
1394
194
決済（通知）レポート
決済（通知）レポート
決済通知
権利管理用クリアリングハウス
電子決済用クリアリングハウス
950
951
ペイメントゲートウェイ
90
利用明細書
少額決済
決済機関
91

【図１０７】

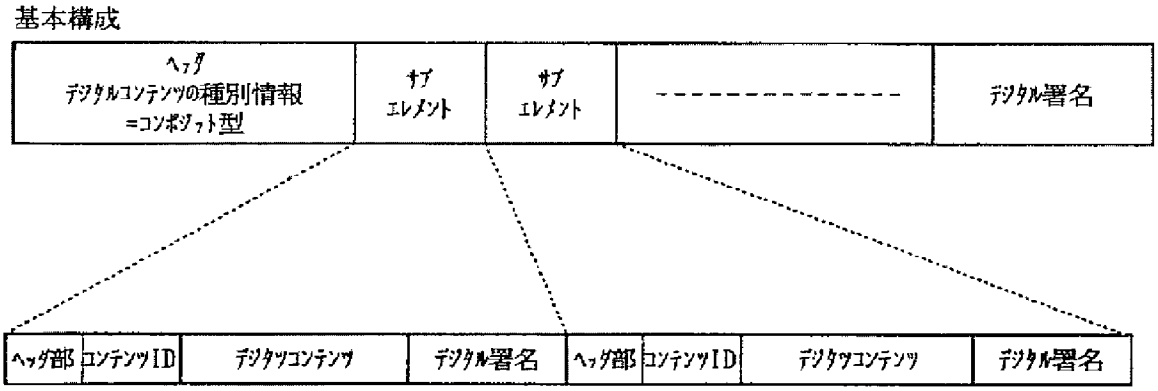

301
310
303a ユーザホームネットワーク
303b
CA
311
SAM
305₁
305₂
305₃
305₄
1394
194
決済（通知）レポート
決済（通知）レポート
決済通知
権利管理用クリアリングハウス
電子決済用クリアリングハウス
302
950
951
ペイメントゲートウェイ
90
利用明細書
少額決済
決済機関
91

【図１０９】



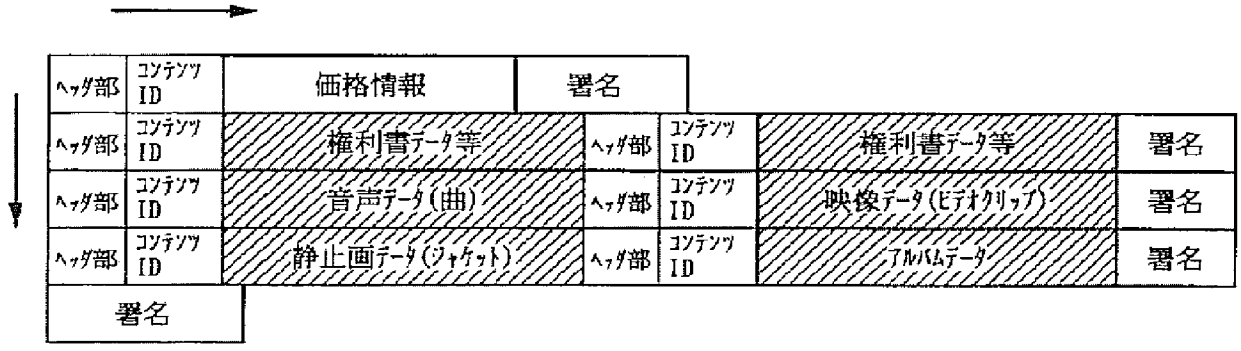
【図１１５】

セキュアコンテナ(コンポジット型)のデータフォーマット－①

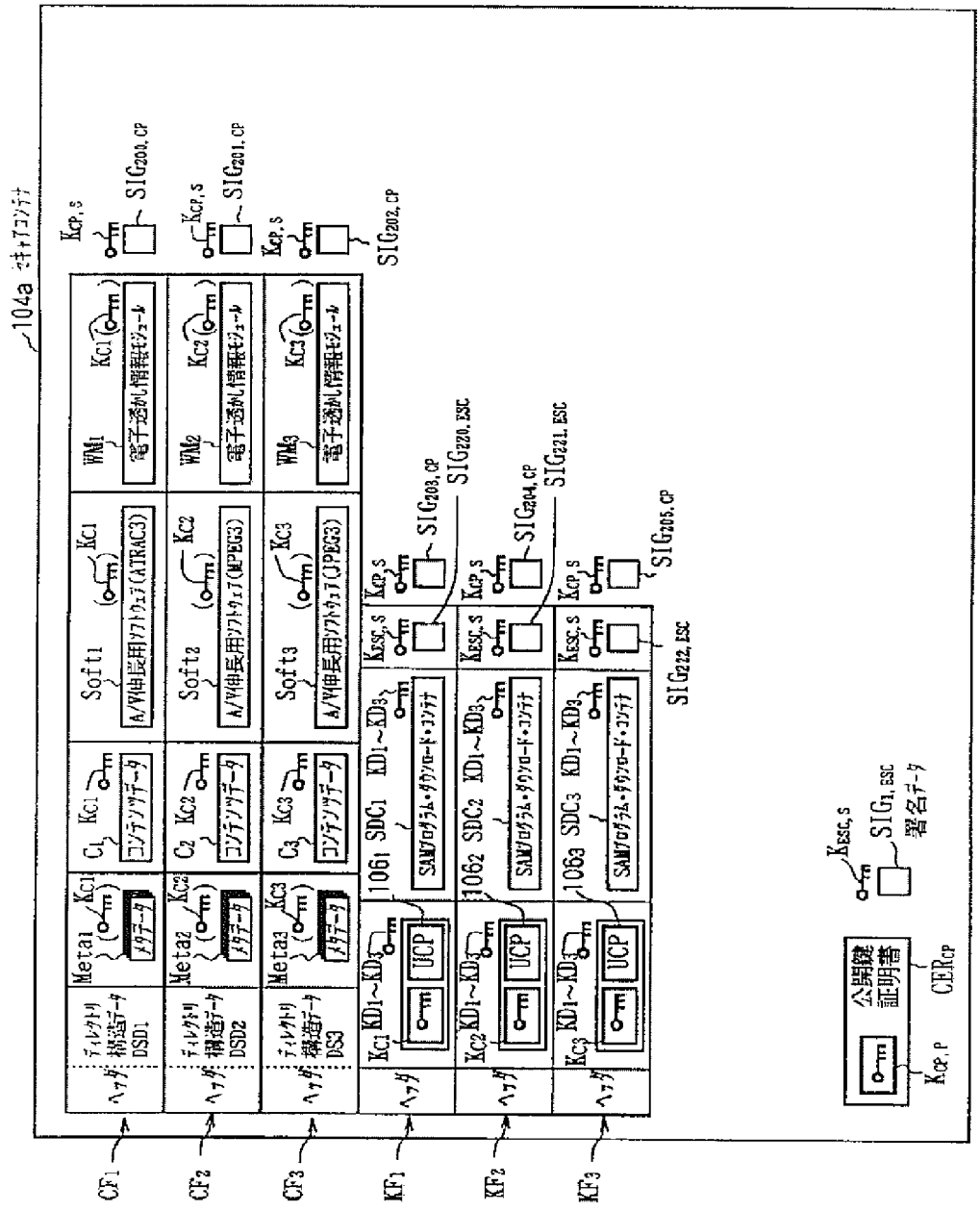


【図１１６】

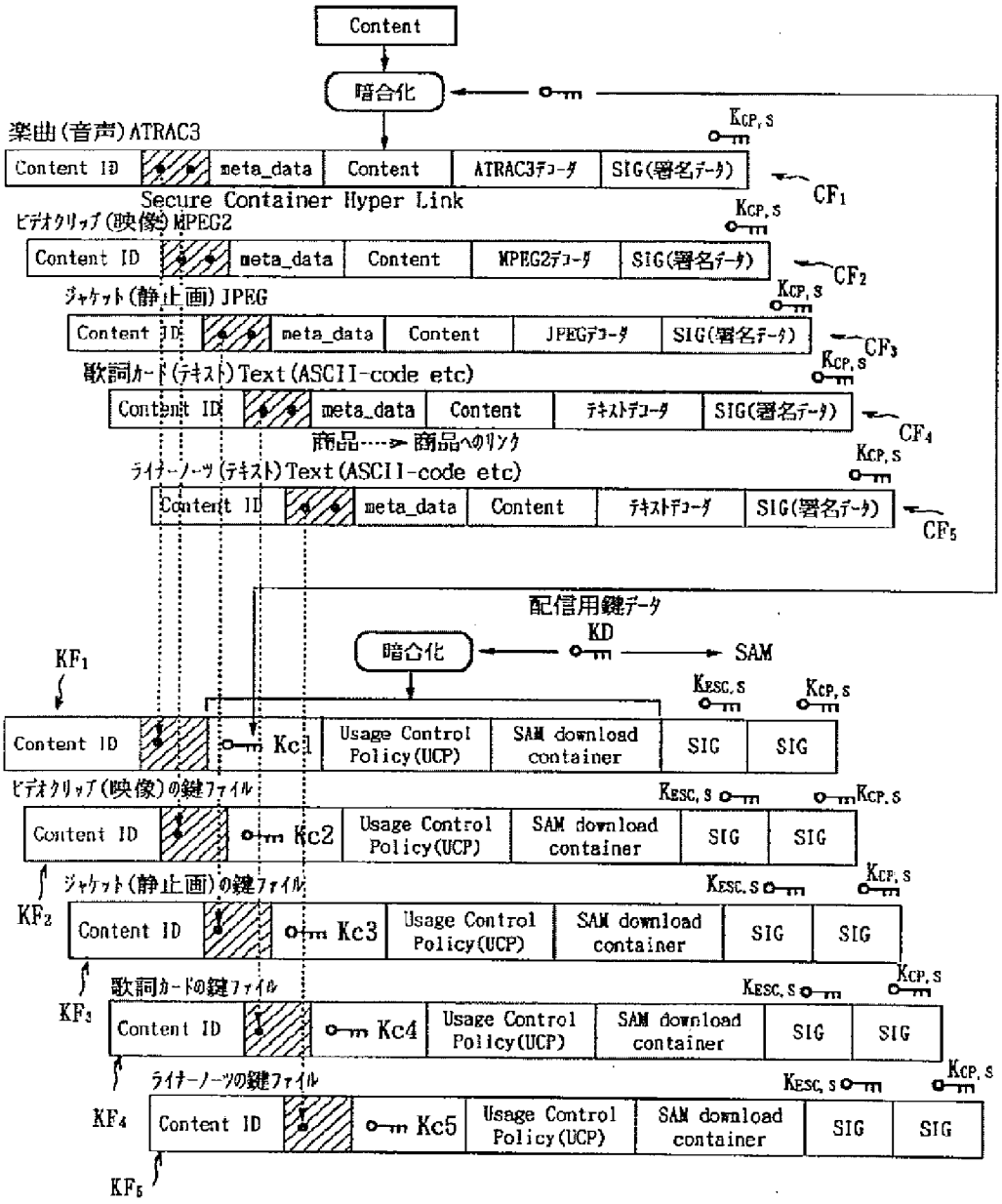
セキュアコンテナ(コンポジット型)のデータフォーマット－②



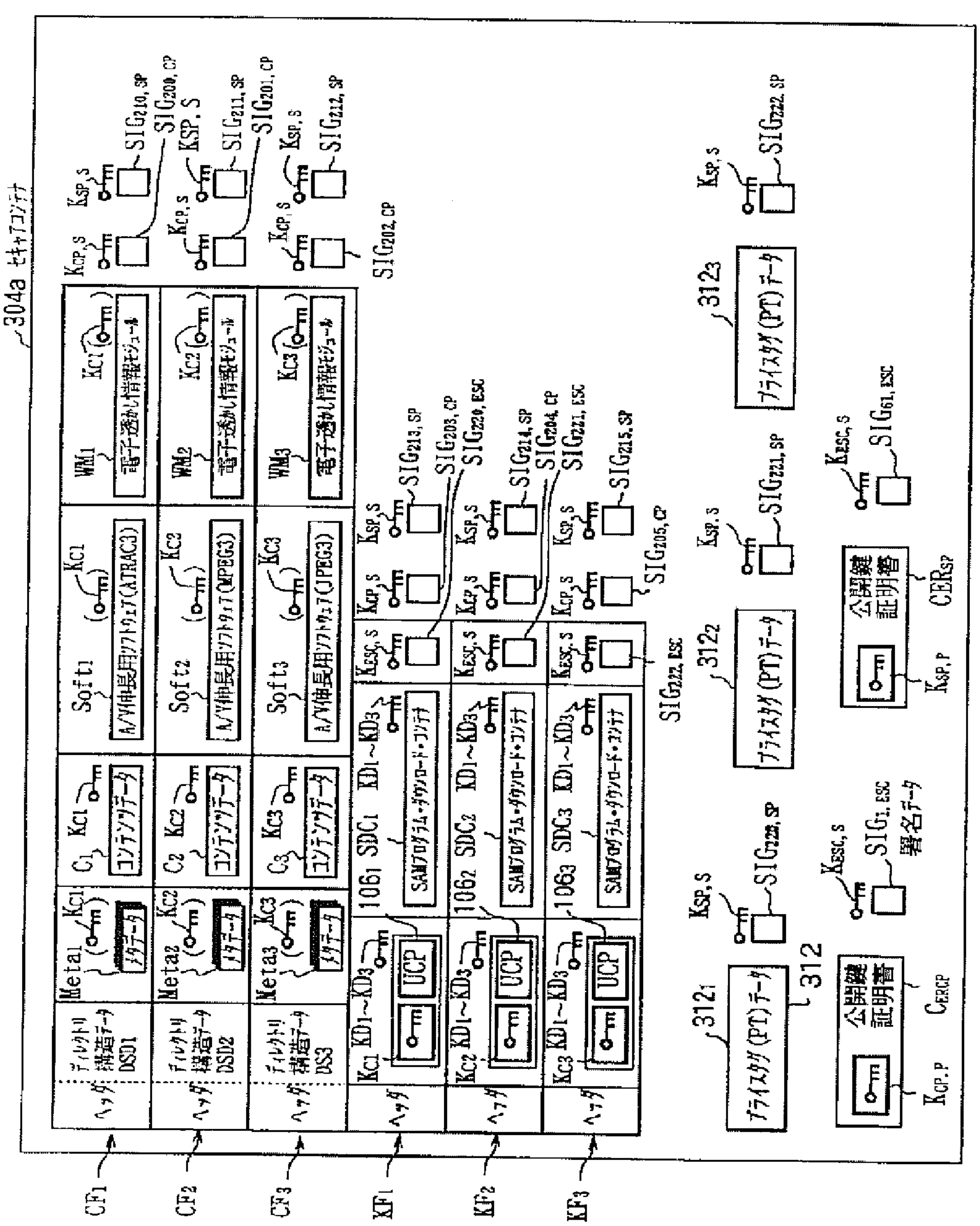
【図１１１】


104a
CF1
CF2
CF3
KF1
KF2
KF3
Meta1
Meta2
Meta3
Soft1
Soft2
Soft3
WM1
WM2
WM3
UCP
SIG200.CP
SIG201.CP
SIG202.CP
SIG203.CP
SIG204.CP
SIG205.CP
SIG220.ESC
SIG221.ESC
SIG222.ESC
SIG1.ESC
署名データ
公開鍵証明書
CERCP

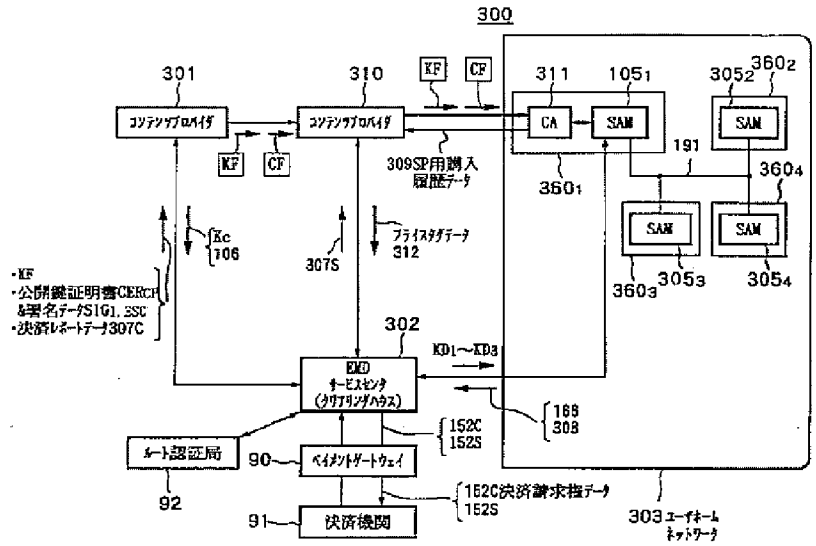
【図１１３】


Content
暗合化
楽曲(音声)ATRAC3
Content ID
meta_data
Content
ATRAC3ﾃﾞｺｰﾀﾞ
SIG(署名ﾃﾞｰﾀ)
Secure Container Hyper Link
ビデオクリップ(映像)MPEG2
MPEG2ﾃﾞｺｰﾀﾞ
ジャケット(静止画)JPEG
JPEGﾃﾞｺｰﾀﾞ
歌詞ｶｰﾄﾞ(ﾃｷｽﾄ)Text(ASCII-code etc)
ﾃｷｽﾄﾃﾞｺｰﾀﾞ
商品⋯➢商品へのリンク
ﾗｲﾅｰﾉｰﾂ(ﾃｷｽﾄ)Text(ASCII-code etc)
CF1
CF2
CF3
CF4
CF5
配信用鍵データ
KD
SAM
KF1
KF2
KF3
KF4
KF5
Kc1
Kc2
Kc3
Kc4
Kc5
Usage Control Policy(UCP)
SAM download container
SIG
ビデオクリップ(映像)の鍵ファイル
ジャケット(静止画)の鍵ファイル
歌詞ｶｰﾄﾞの鍵ファイル
ﾗｲﾅｰﾉｰﾂの鍵ファイル

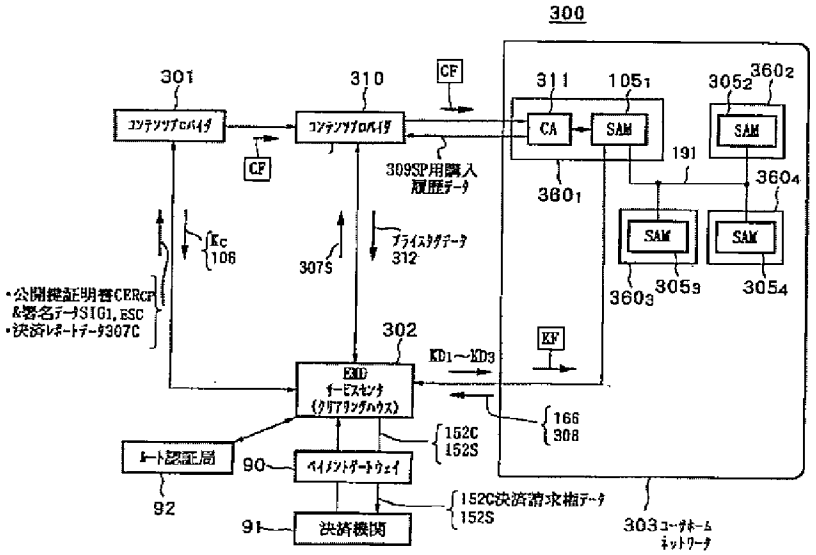
【図１１４】


304a セキュアコンテナ
CF1
CF2
CF3
XF1
XF2
XF3
312
3121
3122
3123
プライスタグ(PT)データ
公開鍵証明書
CERSP
CERCP
署名データ

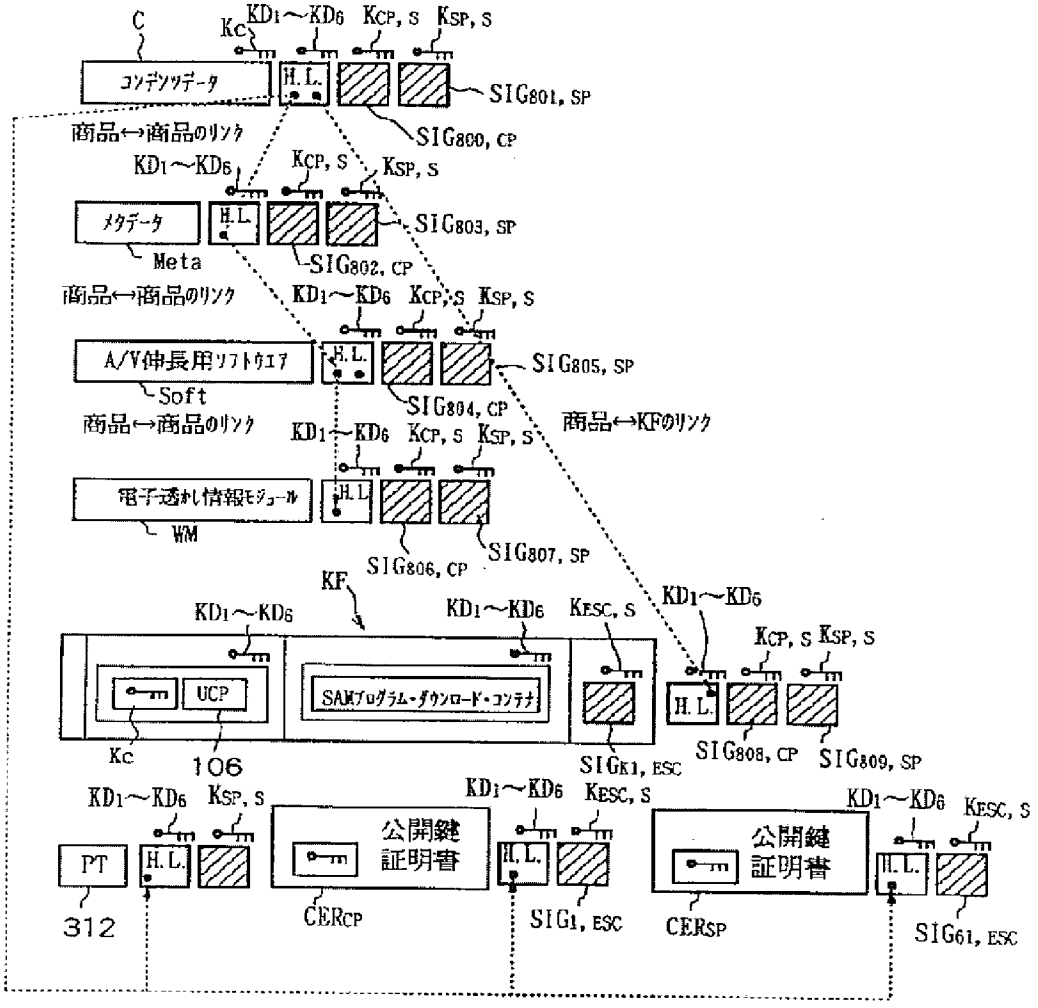
【図１１７】


300
301
310
KF
CF
311
1051
3052
3602
CA
SAM
309SP用購入履歴データ
191
3604
3601
Kc 106
307S
プライスタグデータ 312
3603
3053
3054
・KF
・公開鍵証明書CERCH &署名データSIG1, ESC
・決済レポートデータ307C
302
KD1～KD3
EMD サービスセンタ (クリアリングハウス)
166 308
152C 152S
ルート認証局
90
ペイメントゲートウェイ
92
91
決済機関
152C決済請求指示データ 152S
303ユーザホームネットワーク

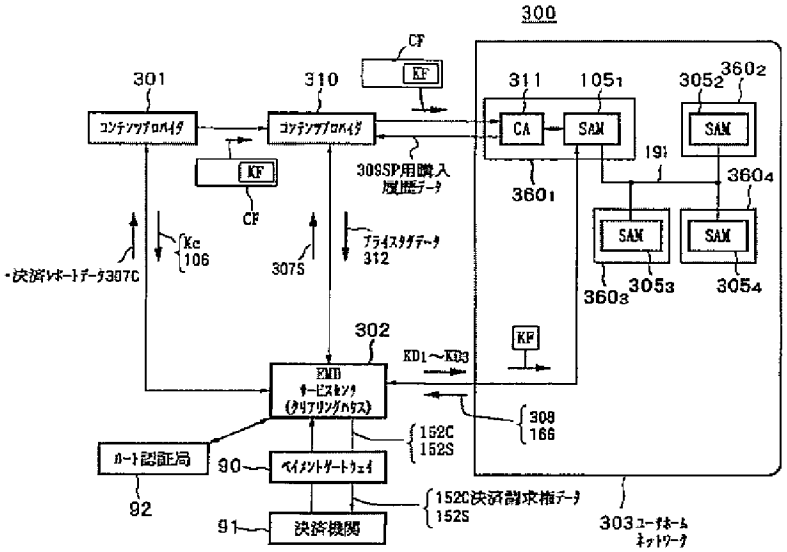
【図１１８】


300
301
310
CF
311
1051
3052
3602
CA
SAM
309SP用購入履歴データ
191
3604
3601
Kc 106
307S
プライスタグデータ 312
3603
3053
3054
・公開鍵証明書CERCH &署名データSIG1, ESC
・決済レポートデータ307C
302
KD1～KD3
KF
EMD サービスセンタ (クリアリングハウス)
166 308
152C 152S
ルート認証局
90
ペイメントゲートウェイ
92
91
決済機関
152C決済請求指示データ 152S
303ユーザホームネットワーク

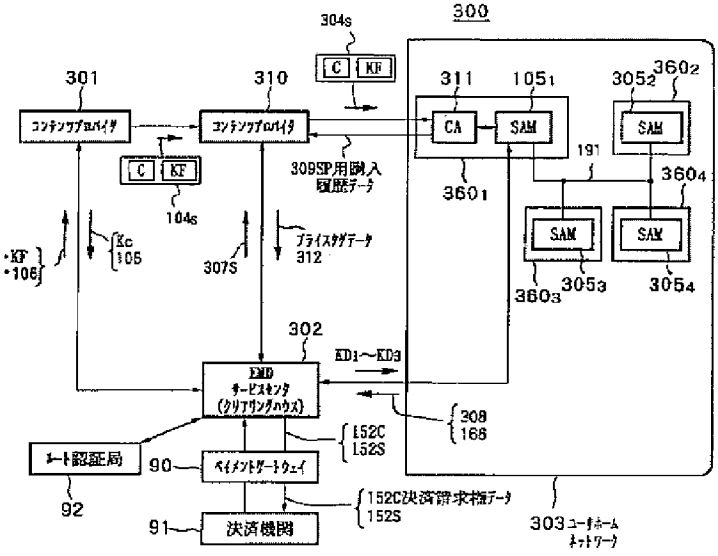
【図１１９】


C
Kc
KD1～KD6
KCP, S
KSP, S
コンテンツデータ
H.L.
SIG801, SP
SIG800, CP
商品↔商品のリンク
メタデータ
Meta
SIG803, SP
SIG802, CP
A/V伸長用ソフトウエア
Soft
SIG805, SP
SIG804, CP
電子透かし情報モジュール
WM
SIG806, CP
SIG807, SP
商品↔KFのリンク
KF
KESC, S
UCP
SAMプログラム・ダウンロード・コンテナ
106
SIGK1, ESC
SIG808, CP
SIG809, SP
PT
312
公開鍵証明書
CERCP
SIG1, ESC
CERSP
SIG61, ESC

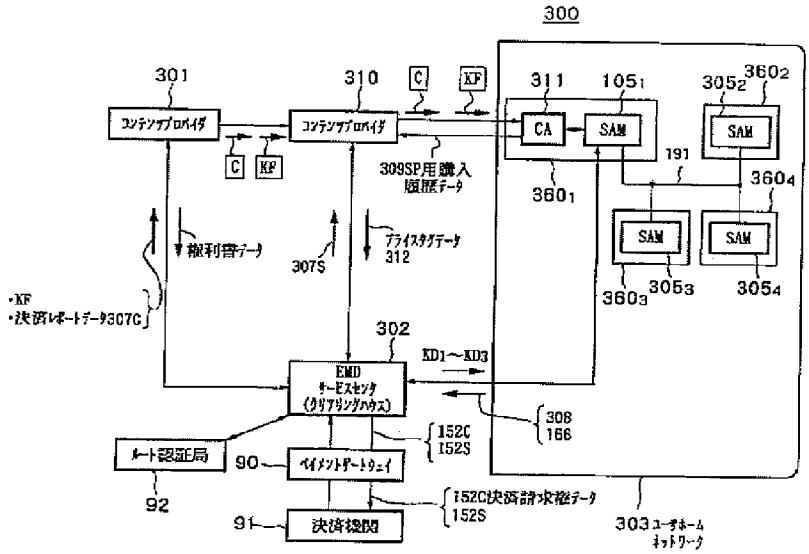
【図１２０】


300
CF
KF
301
310
311
1051
3052
3602
コンテンツプロバイダ
コンテンツプロバイダ
CA
SAM
SAM
KF
CF
309SP用購入履歴データ
191
3601
3604
Kc
106
307S
プライスタグデータ
312
・決済レポートデータ307C
SAM
SAM
SAM
3603
3053
3054
302
KD1～KD3
KF
EMD
サービスセンタ
(クリアリングハウス)
309
166
152C
152S
ルート認証局
90
ペイメントゲートウェイ
92
91
決済機関
152C決済請求権データ
152S
303ユーザホーム
ネットワーク

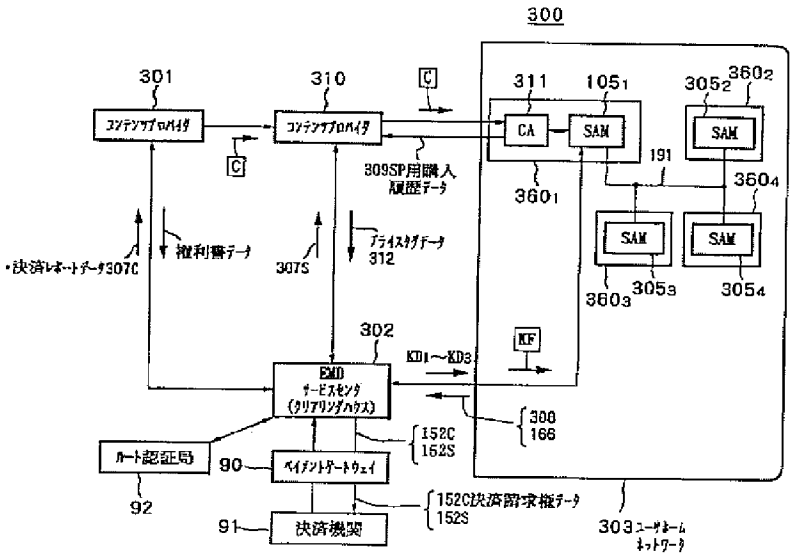
【図１２１】


300
304s
C
KF
301
310
311
1051
3052
3602
コンテンツプロバイダ
コンテンツプロバイダ
CA
SAM
SAM
C
KF
309SP用購入履歴データ
191
3601
3604
104s
・KF
・106
Kc
105
307S
プライスタグデータ
312
SAM
SAM
SAM
3603
3053
3054
302
KD1～KD3
EMD
サービスセンタ
(クリアリングハウス)
309
168
152C
152S
ルート認証局
90
ペイメントゲートウェイ
92
91
決済機関
152C決済請求権データ
152S
303ユーザホーム
ネットワーク

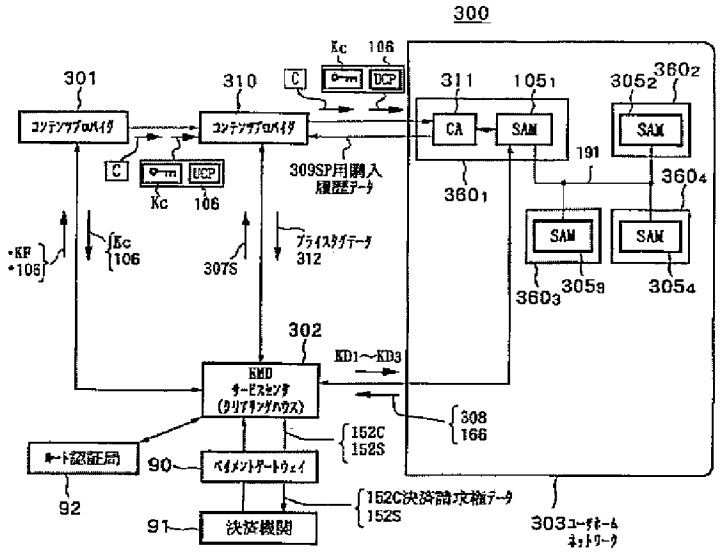
【図１２２】


300
301
310
C
KF
311
105_1
305_2
360_2
コンテンツプロバイダ
コンテンツプロバイダ
CA
SAM
SAM
191
309SP用購入履歴データ
360_1
360_4
SAM
SAM
SAM
権利書データ
307S
プライスタグデータ312
360_3
305_3
305_4
・KF
・決済レポートデータ307C
302
KD1～KD3
EMD
サービスセンタ
(クリアリングハウス)
308
166
152C
152S
カード認証局
90
ペイメントゲートウェイ
92
152C決済請求権データ
152S
91
決済機関
303ユーザホーム
ネットワーク

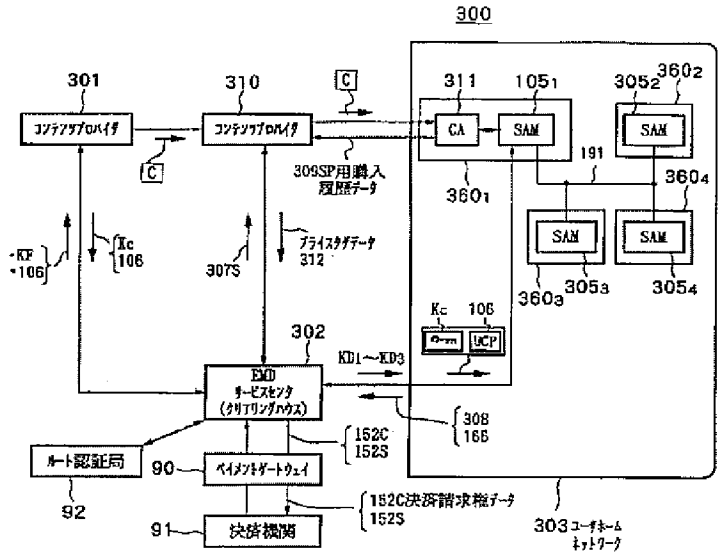
【図１２３】


300
301
310
C
311
105_1
305_2
360_2
コンテンツプロバイダ
コンテンツプロバイダ
CA
SAM
SAM
191
309SP用購入履歴データ
360_1
360_4
SAM
SAM
SAM
・決済レポートデータ307C
権利書データ
307S
プライスタグデータ312
360_3
305_3
305_4
302
KF
KD1～KD3
EMD
サービスセンタ
(クリアリングハウス)
308
166
152C
152S
カード認証局
90
ペイメントゲートウェイ
92
152C決済請求権データ
152S
91
決済機関
303ユーザホーム
ネットワーク

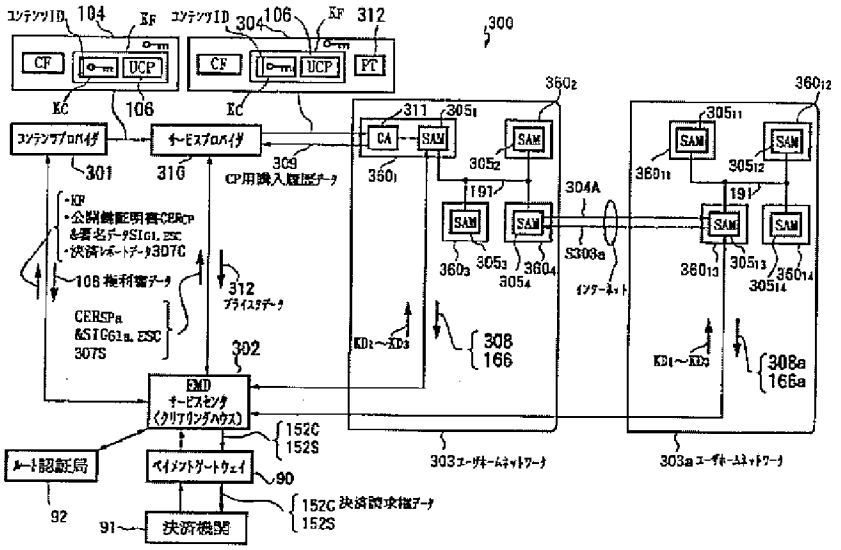
【図１２４】


300
301
310
C
Kc 106
DCP
311
105₁
3052
360₂
コンテンツプロバイダ
コンテンツプロバイダ
CA
SAM
SAM
191
C
UCP
Kc 106
309SP用購入履歴データ
360₁
360₄
SAM
SAM
KF 106
Kc 106
307S
プライスタグデータ 312
360₃
305₃
305₄
302
KD1～KD3
KMD サービスセンタ (クリアリングハウス)
308 166
152C 152S
カード認証局
90
ペイメントゲートウェイ
92
152C決済請求権データ 152S
91
決済機関
303ユーザホームネットワーク

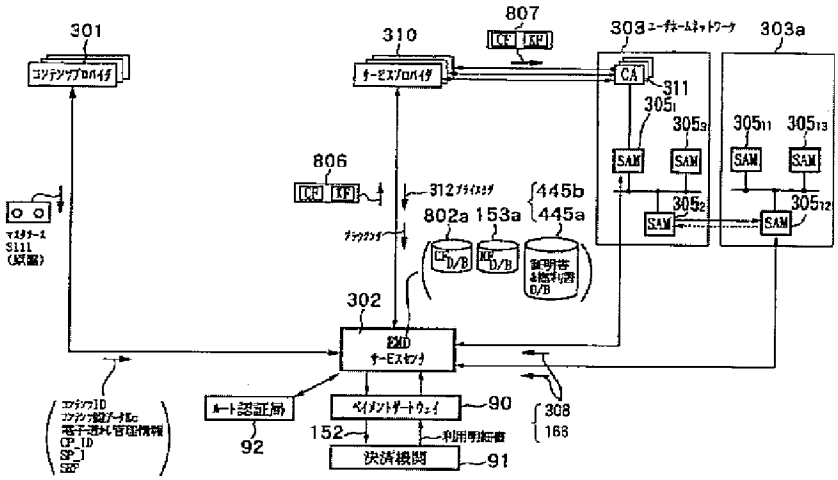
【図１２５】


300
301
310
C
311
105₁
3052
360₂
コンテンツプロバイダ
コンテンツプロバイダ
CA
SAM
SAM
C
191
309SP用購入履歴データ
360₁
360₄
SAM
SAM
KF 106
Kc 106
307S
プライスタグデータ 312
360₃
305₃
305₄
Kc 106
UCP
302
KD1～KD3
KMD サービスセンタ (クリアリングハウス)
308 166
152C 152S
カード認証局
90
ペイメントゲートウェイ
92
152C決済請求権データ 152S
91
決済機関
303ユーザホームネットワーク

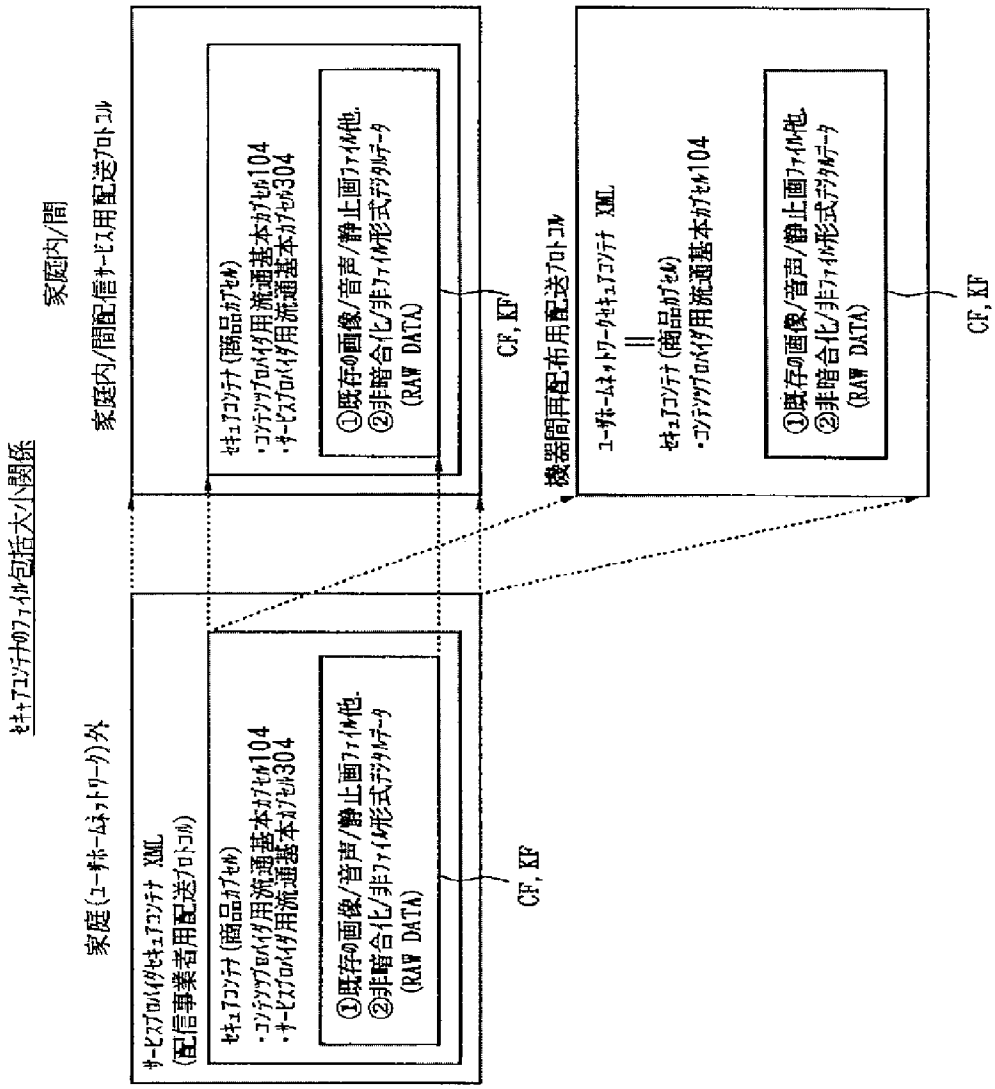
【図１２６】


コンテンツID
104
KF
コンテンツID
304
106
KF
312
300
CF
UCP
CF
UCP
PT
KC
106
KC
コンテンツプロバイダ
サービスプロバイダ
301
310
309
CP用購入履歴データ
CA
SAM
311
305₁
360₂
360₁₂
305₂
191
304A
360₃
305₃
360₄
305₄
S303a
インターネット
360₁₁
305₁₁
305₁₂
360₁₃
305₁₃
360₁₄
305₁₄
・KF
・公開鍵証明書CERCP
&署名データSIG1, ESC
・決済レポートデータ307C
108 権利書データ
312
プライスデータ
CERSPB
&SIG61B, ESC
307S
302
KD₁～KD₃
308
166
308a
166a
END
サービスセンタ
(クリアリングハウス)
152C
152S
ルート認証局
ペイメントゲートウェイ
90
92
91
決済機関
152C 決済請求指示データ
152S
303ユーザホームネットワーク
303aユーザホームネットワーク

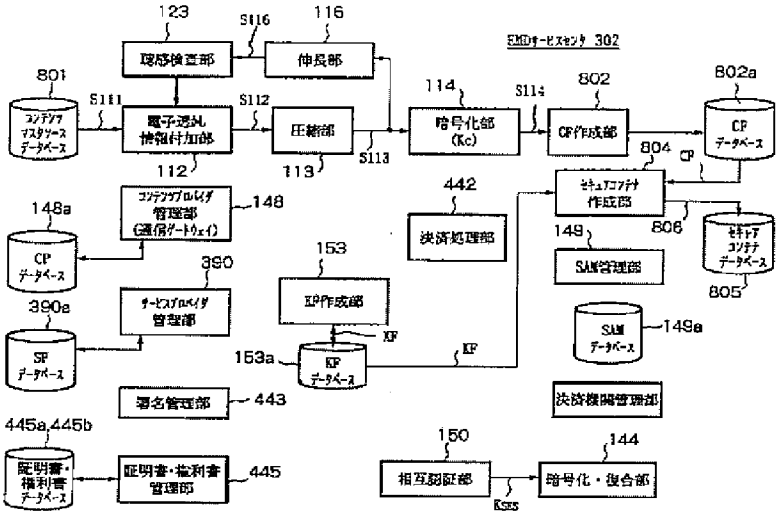
【図１２８】


301
コンテンツプロバイダ
310
サービスプロバイダ
807
CF
KF
303ユーザホームネットワーク
303a
CA
311
305₁
305₃
305₁₁
305₁₃
SAM
305₂
305₁₂
806
CF
KF
312プライスデータ
445b
445a
802a
153a
CP D/B
KF D/B
証明書&権利書 D/B
302
END
サービスセンタ
ルート認証局
92
ペイメントゲートウェイ
90
152
利用明細書
決済機関
91
308
168

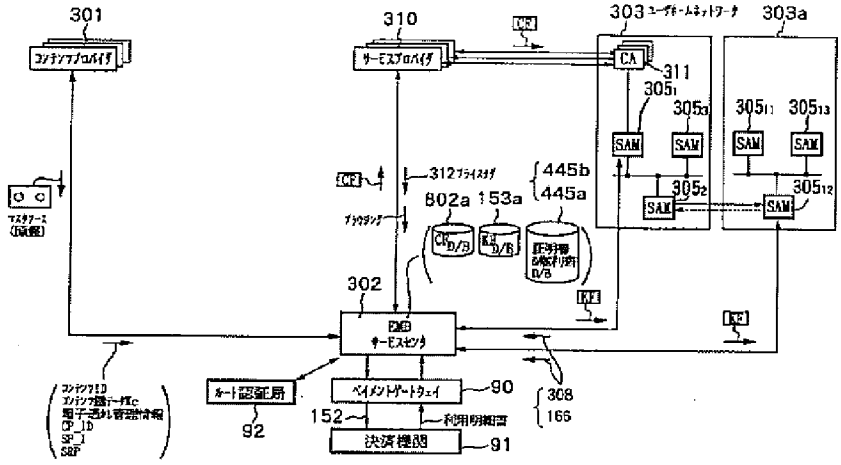
【図１２７】


セキュアコンテナのファイル名括弧大小関係
家庭(ユーザホームネットワーク)外
家庭内/間
家庭内/間配信サービス用配送プロトコル
サービスプロバイダセキュアコンテナ XML
(配信事業者用配送プロトコル)
セキュアコンテナ (商品カプセル)
・コンテンツプロバイダ用流通基本カプセル104
・サービスプロバイダ用流通基本カプセル304
①既存の画像/音声/静止画ファイル他.
②非暗合化/非ファイル形式デジタルデータ
(RAW DATA)
CF, KF
セキュアコンテナ (商品カプセル)
・コンテンツプロバイダ用流通基本カプセル104
・サービスプロバイダ用流通基本カプセル304
①既存の画像/音声/静止画ファイル他.
②非暗合化/非ファイル形式デジタルデータ
(RAW DATA)
CF, KF
機器間用配布用配送プロトコル
ユーザホームネットワークセキュアコンテナ XML
||
セキュアコンテナ (商品カプセル)
・コンテンツプロバイダ用流通基本カプセル104
①既存の画像/音声/静止画ファイル他.
②非暗合化/非ファイル形式デジタルデータ
(RAW DATA)
CF, KF

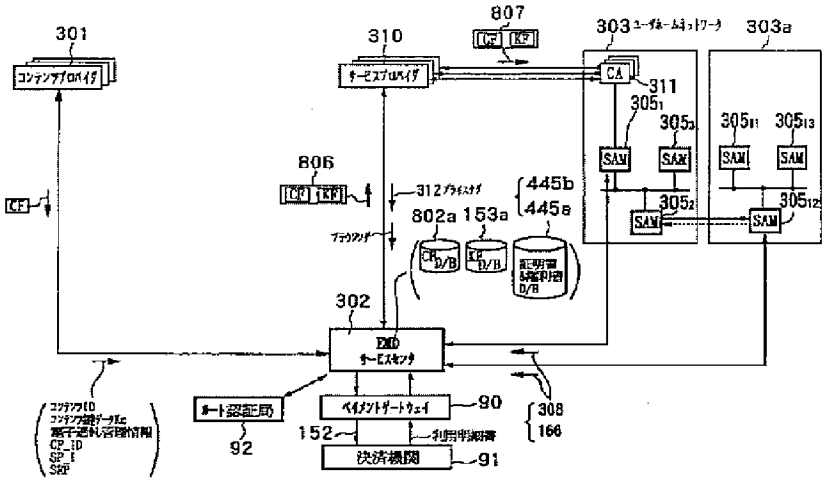
【図１２９】


123
S116
116
端末検査部
伸長部
801
S111
電子透かし情報付加部
S112
圧縮部
112
113
S113
114
暗号化部 (Kc)
S114
802
CP作成部
802a
CP データベース
804
CP
セキュアコンテナ作成部
806
セキュアコンテナデータベース
805
442
決済処理部
149
SAM管理部
149a
SAM データベース
決済機関管理部
148a
CP データベース
148
コンテンツプロバイダ管理部 (通信ゲートウェイ)
390
サービスプロバイダ管理部
390a
SP データベース
153
KP作成部
KF
153a
KP データベース
署名管理部
443
445a,445b
証明書・権利書データベース
証明書・権利書管理部
445
150
相互認証部
Kss
144
暗号化・復合部

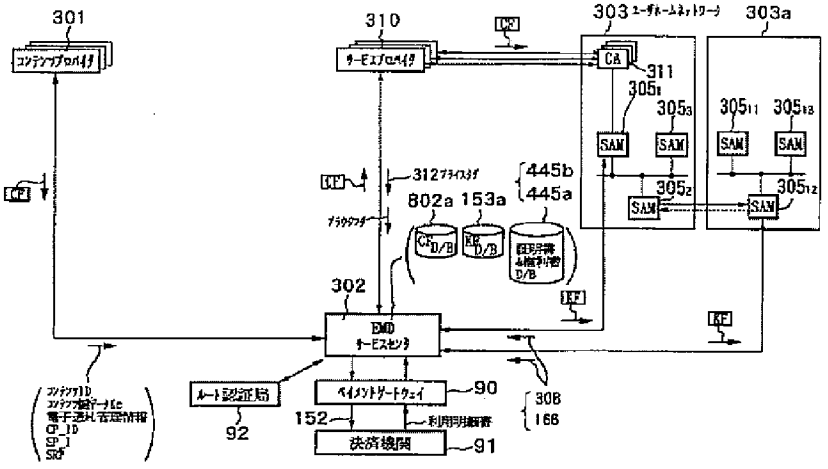
【図１３０】


301
コンテンツプロバイダ
310
サービスプロバイダ
303
303a
CA
311
305₁
305₀
305₁₁
305₁₃
305₂
305₁₂
SAM
CP
312
445b
445a
802a
153a
302
決済機関 サービスセンタ
KF
カード認証局
92
ペイメントゲートウェイ
90
152
利用明細書
決済機関
91
308
165

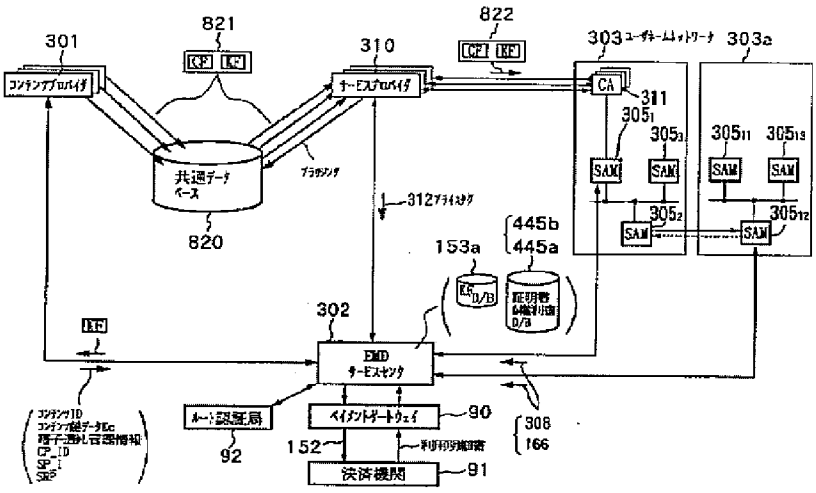
【図１３１】


301
310
807
303
303a
806
312
445b
445a
802a
153a
302
SAM
CA
311
90
91
92
152
308
166

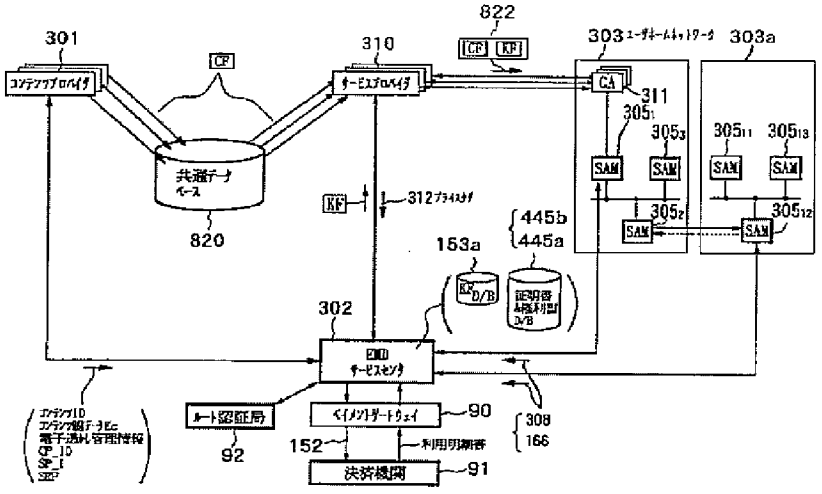
【図１３２】


301
310
303
303a
312
445b
445a
802a
153a
302
SAM
CA
311
90
91
92
152
308
166

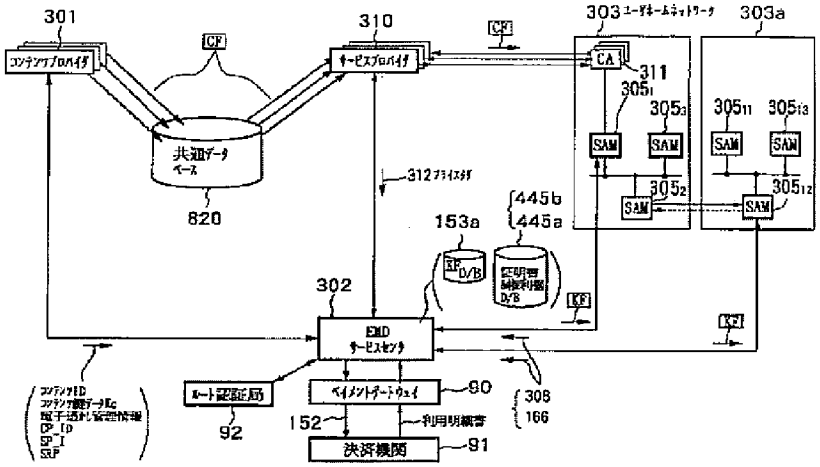
【図１３３】


301
821
822
310
303
303a
CP
KF
CA
311
共通データベース
820
312
445b
445a
153a
302
EMD
90
91
92
152
308
166

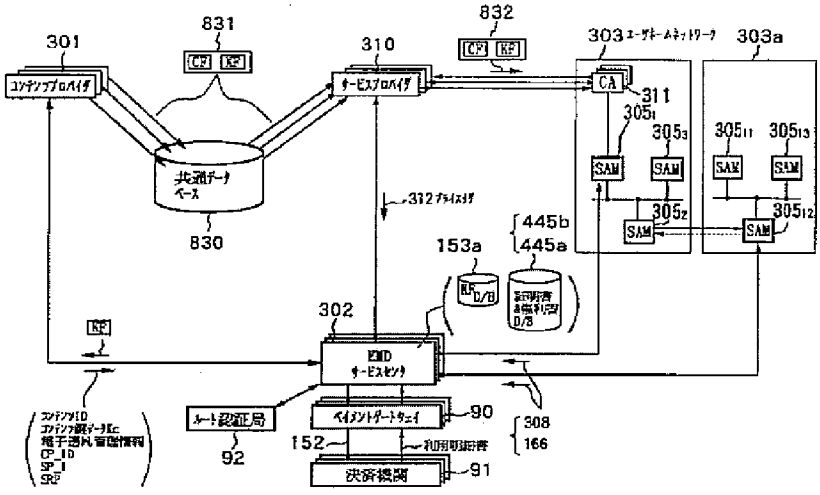
【図１３４】


301
822
310
303
303a
CP
KF
CA
311
共通データベース
820
312
445b
445a
153a
302
EMD
90
91
92
152
308
166

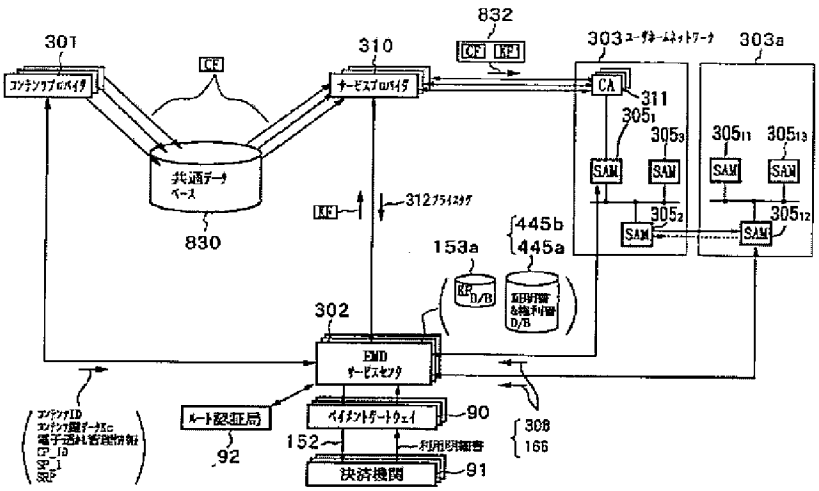
【図１３５】


301
310
303
303a
CP
CA
311
820
312
153a
445b
445a
302
SAM
90
91
92
152
308
166
利用明細書

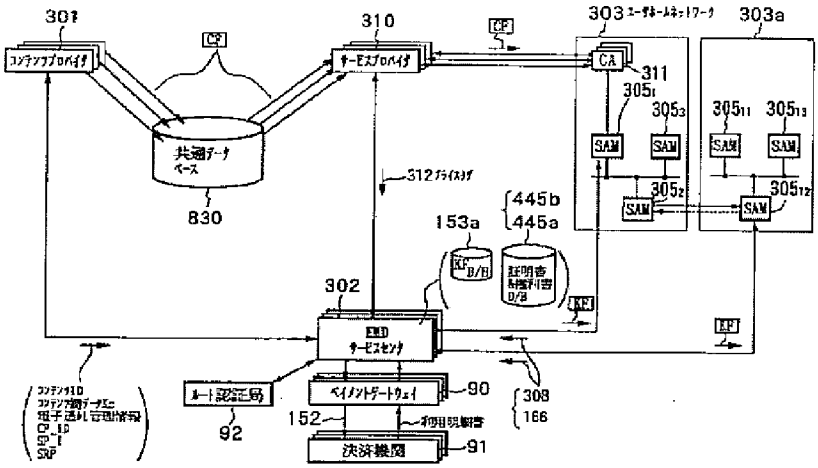
【図１３６】


831
832
301
310
303
303a
CP
KF
CA
311
830
312
153a
445b
445a
302
SAM
90
91
92
152
308
166
利用明細書

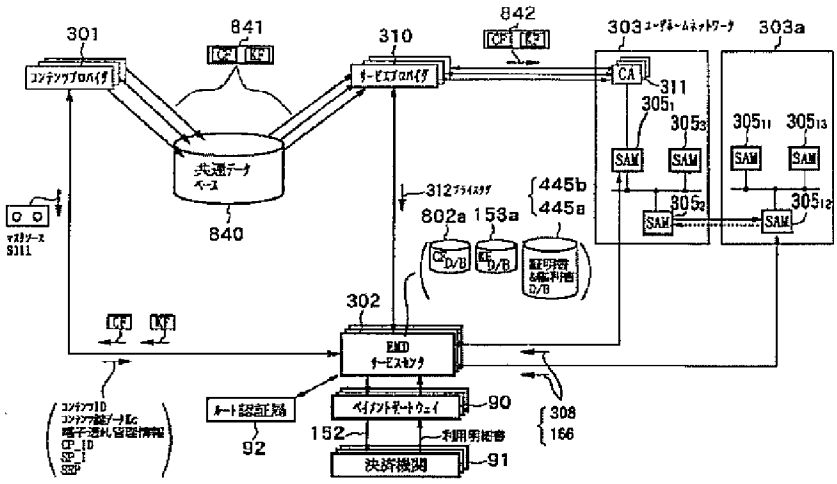
【図１３７】


832
301
310
303
303a
CP
KF
CA
311
SAM
830
312
153a
445b
445a
302
EMD
ペイメントゲートウェイ
90
92
152
91
308
166
決済機関

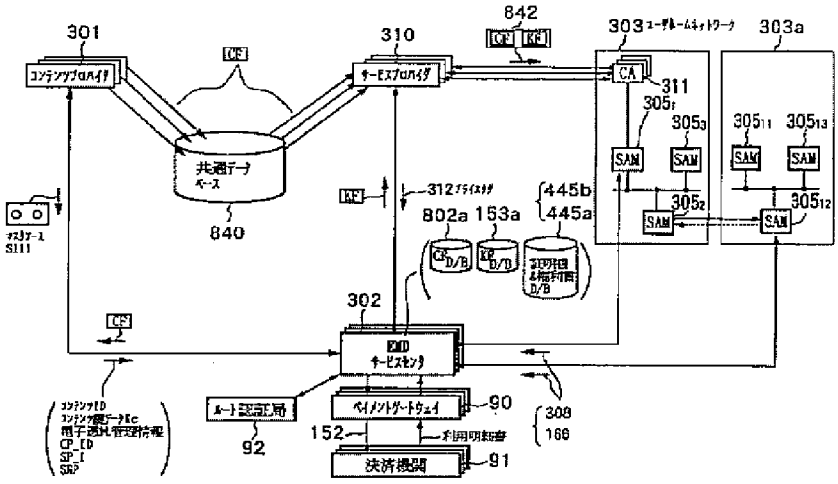
【図１３８】


301
310
303
303a
CP
KF
CA
311
SAM
830
312
153a
445b
445a
302
EMD
ペイメントゲートウェイ
90
92
152
91
308
166
決済機関

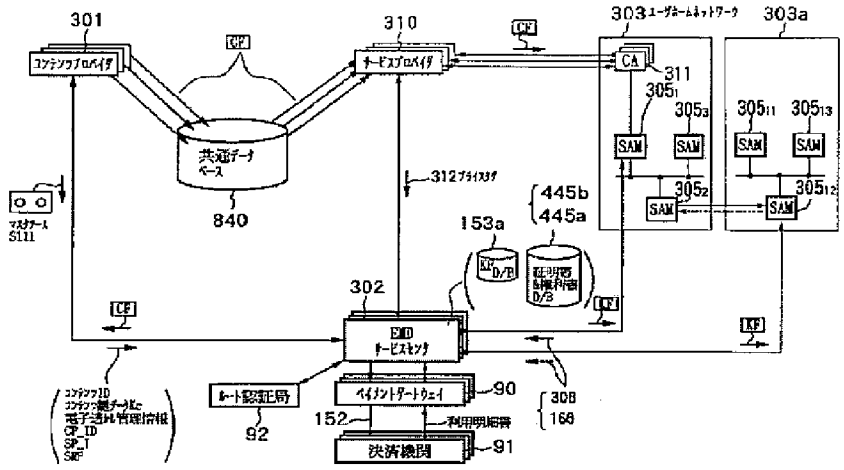
【図１３９】


301
841
310
842
303
303a
311
840
312
445b
445a
802a
153a
302
90
91
92
152
308
166

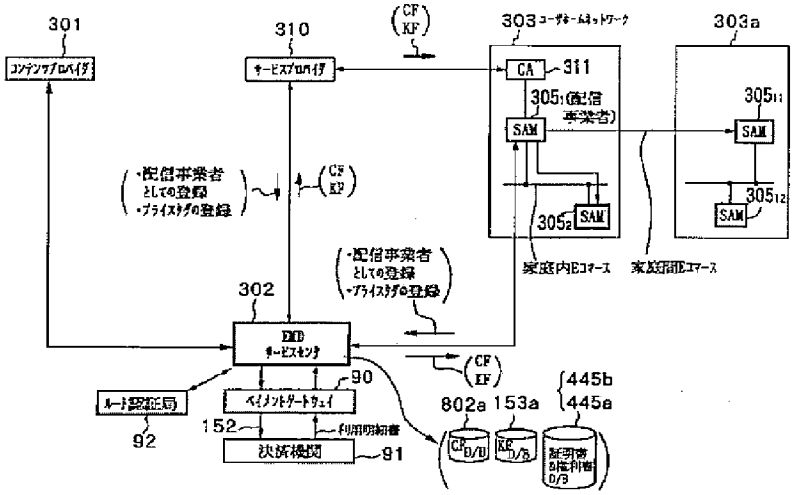
【図１４０】


301
310
842
303
303a
311
840
312
445b
445a
802a
153a
302
90
91
92
152
308
166

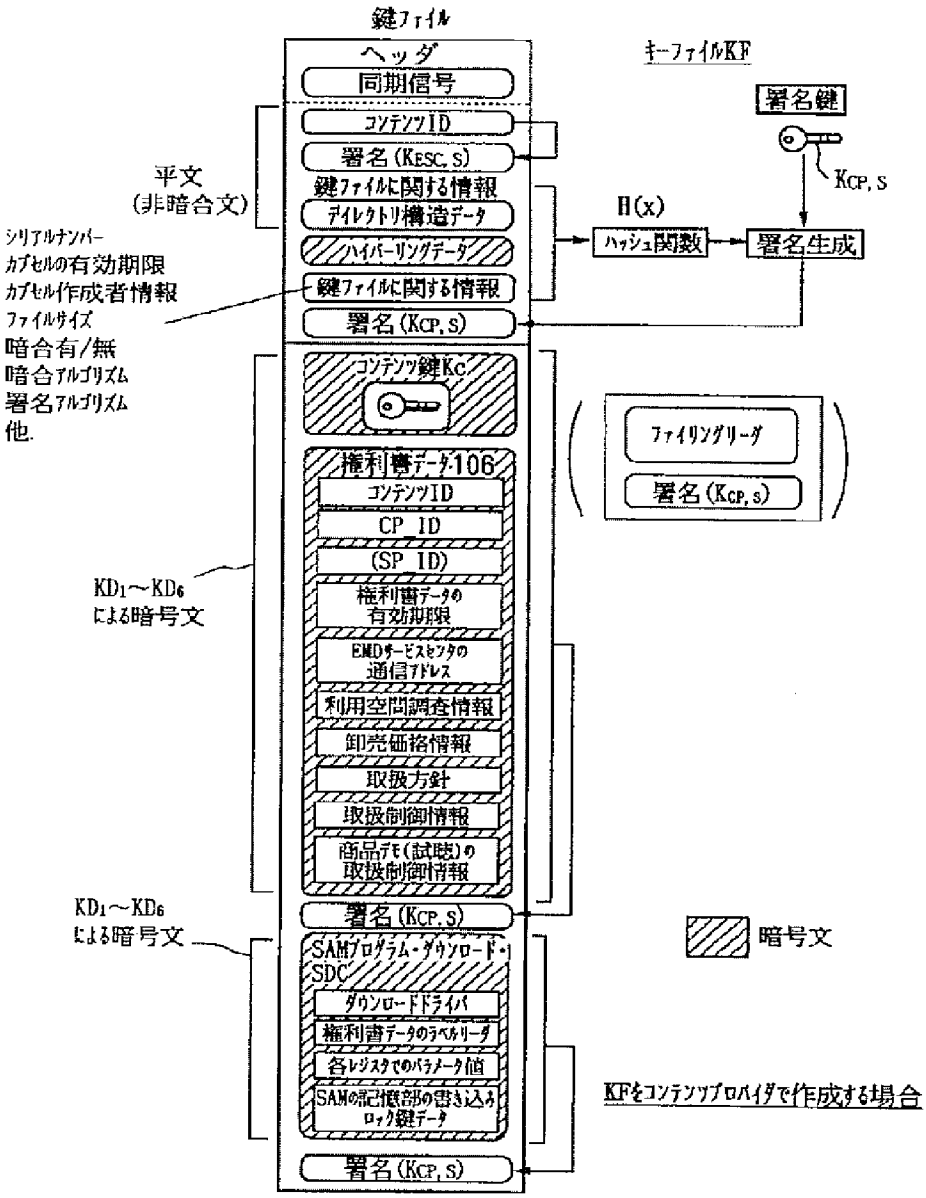
【図１４１】


301
310
303
303a
CA
311
SAM
840
302
90
91
92
152
153a
445b
445a

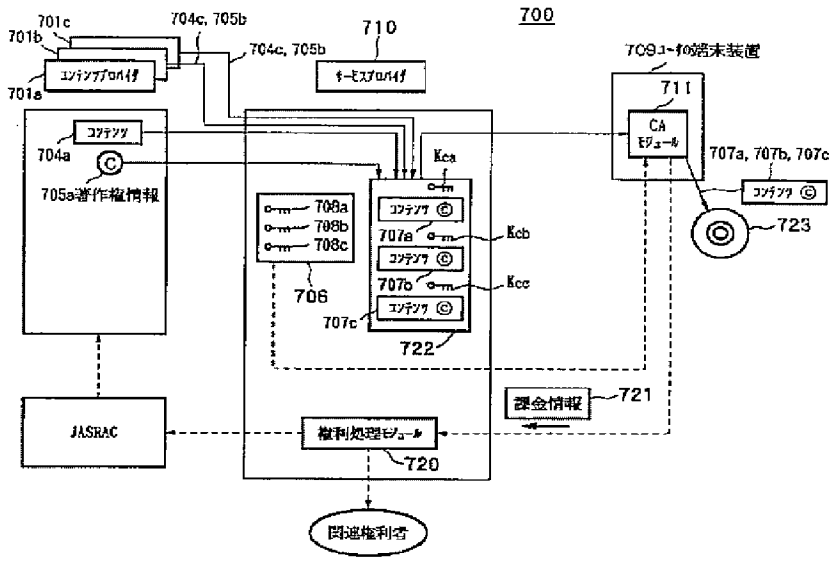
【図１４２】


301
310
303
303a
CA
311
SAM
302
90
91
92
152
153a
445b
445a
802a

【図１４４】


鍵ファイル
ヘッダ
同期信号
コンテンツID
署名(KESC, S)
鍵ファイルに関する情報
ディレクトリ構造データ
ハイパーリングデータ
鍵ファイルに関する情報
署名(KCP, S)
平文
(非暗合文)
シリアルナンバー
カプセルの有効期限
カプセル作成者情報
ファイルサイズ
暗合有/無
暗合アルゴリズム
署名アルゴリズム
他.
H(x)
ハッシュ関数
署名生成
キーファイルKF
署名鍵
KCP, S
コンテンツ鍵Kc
権利書データ106
コンテンツID
CP_ID
(SP_ID)
権利書データの有効期限
EMDサービスセンタの通信アドレス
利用空間調査情報
卸売価格情報
取扱方針
取扱制御情報
商品デモ(試聴)の取扱制御情報
KD1～KD6による暗号文
署名(KCP, S)
KD1～KD6による暗号文
SAMプログラム・ダウンロード・SDC
ダウンロードドライバ
権利書データのラベルリーダ
各レジスタでのパラメータ値
SAMの記憶領域の書き込みロック鍵データ
署名(KCP, S)
ファイリングリーダ
署名(KCP, S)
暗号文
KFをコンテンツプロバイダで作成する場合

【図１４５】



フロントページの続き

(51) Int. Cl.[7]		識別記号	F I		テーマコード（参考）
Ｇ０９Ｃ	1/00	６６０	Ｇ１１Ｂ	20/10	Ｈ
Ｇ１１Ｂ	20/10		Ｈ０４Ｌ	9/00	６０１Ｃ
Ｈ０４Ｌ	9/32				６７５Ｂ
					６７５Ｄ

Ｆターム（参考）　5B017 AA06 BA05 BA07 BB03 BB10
CA11 CA12 CA16
5B085 AE13 AE29 BG07
5D044 AB05 DE17 GK17 HL11
5J104 AA01 AA09 AA16 EA02 EA04
LA03 LA06 MA02 NA03 PA07
PA10
9A001 BB03 BB04 EE02 EE03 EE04
JJ07 JJ13 LL03

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成18年4月27日(2006.4.27)

【公開番号】特開2001-94549(P2001-94549A)
【公開日】平成13年4月6日(2001.4.6)
【出願番号】特願平11-309721
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
Ｇ０６Ｆ　12/14　(2006.01)
Ｇ０６Ｆ　21/00　(2006.01)
Ｇ０９Ｃ　1/00　(2006.01)
Ｇ１１Ｂ　20/10　(2006.01)
Ｈ０４Ｌ　9/32　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｃ
Ｇ０６Ｆ　12/14　３２０Ｂ
Ｇ０６Ｆ　15/00　３３０Ｚ
Ｇ０９Ｃ　1/00　６４０Ｂ
Ｇ０９Ｃ　1/00　６４０Ｚ
Ｇ０９Ｃ　1/00　６６０Ｄ
Ｇ１１Ｂ　20/10　Ｈ
Ｈ０４Ｌ　9/00　６７５Ｂ
Ｈ０４Ｌ　9/00　６７５Ｄ

【手続補正書】
【提出日】平成18年3月10日(2006.3.10)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、
前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、
前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化された前記コンテンツデータを提供し、
前記データ処理装置は、前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する
データ提供システム。
【請求項２】
前記管理装置は、前記キーファイルの作成者の正当性を検証するための署名データを前記キーファイルに付加する
請求項１に記載のデータ提供システム。
【請求項３】
前記データ提供装置は、前記コンテンツデータを格納したコンテンツファイルを作成し

、当該コンテンツファイルを前記データ処理装置に提供する
請求項１に記載のデータ提供システム。
【請求項４】
前記データ提供装置は、前記権利書データを作成して前記管理装置に送り、
前記データ処理装置は、前記権利書データに基づいて、前記配給を受けたコンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、
前記管理装置は、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置の関係者に分配するための利益分配処理を行う
請求項１に記載のデータ提供システム。
【請求項５】
データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供システムにおいて、
前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、
前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から受けた前記キーファイルとを格納したモジュールを、前記データ処理装置に配給し、
前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する
データ提供システム。
【請求項６】
前記管理装置は、前記キーファイルの作成者の正当性を検証するための署名データを生成し、当該署名データをさらに格納した前記キーファイルを作成する
請求項５に記載のデータ提供システム。
【請求項７】
前記データ提供装置は、前記コンテンツ鍵データおよび前記権利書データを生成して前記管理装置に送信し、
前記管理装置は、受信した前記コンテンツ鍵データおよび前記権利書データに基づいて前記キーファイルを作成し、当該作成したキーファイルを登録する
請求項５に記載のデータ提供システム。
【請求項８】
前記管理装置は、配信用鍵データを用いて暗号化した前記コンテンツ鍵データおよび前記権利書データを格納した前記キーファイルを作成し、
前記配信用鍵データを前記データ処理装置に配給する
請求項５に記載のデータ提供システム。
【請求項９】
データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、
前記管理装置は、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、
前記データ提供装置は、前記コンテンツ鍵データを用いて暗号化された前記コンテンツデータを提供し、
前記データ処理装置は、前記キーファイルに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する
データ提供方法。
【請求項１０】

データ提供装置からデータ処理装置にコンテンツデータを配給し、管理装置によって前記データ提供装置および前記データ処理装置を管理するデータ提供方法において、
前記管理装置において、暗号化されたコンテンツ鍵データと前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したキーファイルを作成し、
前記作成したキーファイルを前記管理装置から前記データ提供装置に配給し、
前記コンテンツ鍵データを用いて暗号化されたコンテンツデータを格納したコンテンツファイルと、前記管理装置から配給を受けた前記キーファイルとを格納したモジュールを前記データ提供装置から前記データ処理装置に配給し、
前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する
データ提供方法。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００１５
【補正方法】削除
【補正の内容】
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００１６
【補正方法】削除
【補正の内容】
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】００１７
【補正方法】削除
【補正の内容】
【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００１８
【補正方法】削除
【補正の内容】
【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】００１９
【補正方法】削除
【補正の内容】
【手続補正７】
【補正対象書類名】明細書
【補正対象項目名】００２０
【補正方法】削除
【補正の内容】
【手続補正８】
【補正対象書類名】明細書
【補正対象項目名】００２１
【補正方法】削除
【補正の内容】
【手続補正９】
【補正対象書類名】明細書
【補正対象項目名】００２２

【補正方法】削除
【補正の内容】
【手続補正１０】
【補正対象書類名】明細書
【補正対象項目名】００２３
【補正方法】削除
【補正の内容】
【手続補正１１】
【補正対象書類名】明細書
【補正対象項目名】００２４
【補正方法】削除
【補正の内容】
【手続補正１２】
【補正対象書類名】明細書
【補正対象項目名】００２５
【補正方法】削除
【補正の内容】
【手続補正１３】
【補正対象書類名】明細書
【補正対象項目名】００２６
【補正方法】削除
【補正の内容】
【手続補正１４】
【補正対象書類名】明細書
【補正対象項目名】００２７
【補正方法】削除
【補正の内容】
【手続補正１５】
【補正対象書類名】明細書
【補正対象項目名】００２８
【補正方法】削除
【補正の内容】
【手続補正１６】
【補正対象書類名】明細書
【補正対象項目名】００２９
【補正方法】削除
【補正の内容】
【手続補正１７】
【補正対象書類名】明細書
【補正対象項目名】００３０
【補正方法】削除
【補正の内容】
【手続補正１８】
【補正対象書類名】明細書
【補正対象項目名】００３１
【補正方法】削除
【補正の内容】
【手続補正１９】
【補正対象書類名】明細書
【補正対象項目名】００３２

【補正方法】削除
【補正の内容】
【手続補正２０】
【補正対象書類名】明細書
【補正対象項目名】００３３
【補正方法】削除
【補正の内容】
【手続補正２１】
【補正対象書類名】明細書
【補正対象項目名】００３４
【補正方法】削除
【補正の内容】
【手続補正２２】
【補正対象書類名】明細書
【補正対象項目名】００３５
【補正方法】削除
【補正の内容】
【手続補正２３】
【補正対象書類名】明細書
【補正対象項目名】００３６
【補正方法】削除
【補正の内容】
【手続補正２４】
【補正対象書類名】明細書
【補正対象項目名】００３７
【補正方法】削除
【補正の内容】
【手続補正２５】
【補正対象書類名】明細書
【補正対象項目名】００３８
【補正方法】削除
【補正の内容】
【手続補正２６】
【補正対象書類名】明細書
【補正対象項目名】００３９
【補正方法】削除
【補正の内容】
【手続補正２７】
【補正対象書類名】明細書
【補正対象項目名】００４０
【補正方法】削除
【補正の内容】
【手続補正２８】
【補正対象書類名】明細書
【補正対象項目名】００４１
【補正方法】削除
【補正の内容】
【手続補正２９】
【補正対象書類名】明細書
【補正対象項目名】００４２

【補正方法】削除
【補正の内容】
【手続補正３０】
【補正対象書類名】明細書
【補正対象項目名】００４３
【補正方法】削除
【補正の内容】
【手続補正３１】
【補正対象書類名】明細書
【補正対象項目名】００４４
【補正方法】削除
【補正の内容】
【手続補正３２】
【補正対象書類名】明細書
【補正対象項目名】００４５
【補正方法】削除
【補正の内容】
【手続補正３３】
【補正対象書類名】明細書
【補正対象項目名】００４６
【補正方法】削除
【補正の内容】
【手続補正３４】
【補正対象書類名】明細書
【補正対象項目名】００４７
【補正方法】削除
【補正の内容】
【手続補正３５】
【補正対象書類名】明細書
【補正対象項目名】００４８
【補正方法】削除
【補正の内容】
【手続補正３６】
【補正対象書類名】明細書
【補正対象項目名】００４９
【補正方法】削除
【補正の内容】
【手続補正３７】
【補正対象書類名】明細書
【補正対象項目名】００５０
【補正方法】削除
【補正の内容】
【手続補正３８】
【補正対象書類名】明細書
【補正対象項目名】００５１
【補正方法】削除
【補正の内容】
【手続補正３９】
【補正対象書類名】明細書
【補正対象項目名】００５２

【補正方法】削除
【補正の内容】
【手続補正４０】
【補正対象書類名】明細書
【補正対象項目名】００５３
【補正方法】削除
【補正の内容】
【手続補正４１】
【補正対象書類名】明細書
【補正対象項目名】００５４
【補正方法】削除
【補正の内容】
【手続補正４２】
【補正対象書類名】明細書
【補正対象項目名】００５５
【補正方法】削除
【補正の内容】
【手続補正４３】
【補正対象書類名】明細書
【補正対象項目名】００５８
【補正方法】削除
【補正の内容】
【手続補正４４】
【補正対象書類名】明細書
【補正対象項目名】００５９
【補正方法】削除
【補正の内容】
【手続補正４５】
【補正対象書類名】明細書
【補正対象項目名】００６０
【補正方法】削除
【補正の内容】
【手続補正４６】
【補正対象書類名】明細書
【補正対象項目名】００６１
【補正方法】削除
【補正の内容】
【手続補正４７】
【補正対象書類名】明細書
【補正対象項目名】００６２
【補正方法】削除
【補正の内容】
【手続補正４８】
【補正対象書類名】明細書
【補正対象項目名】００６３
【補正方法】削除
【補正の内容】
【手続補正４９】
【補正対象書類名】明細書
【補正対象項目名】００６４

【補正方法】削除
【補正の内容】
【手続補正５０】
【補正対象書類名】明細書
【補正対象項目名】００６５
【補正方法】削除
【補正の内容】
【手続補正５１】
【補正対象書類名】明細書
【補正対象項目名】００６６
【補正方法】削除
【補正の内容】
【手続補正５２】
【補正対象書類名】明細書
【補正対象項目名】００６７
【補正方法】削除
【補正の内容】
【手続補正５３】
【補正対象書類名】明細書
【補正対象項目名】００６８
【補正方法】削除
【補正の内容】
【手続補正５４】
【補正対象書類名】明細書
【補正対象項目名】００６９
【補正方法】削除
【補正の内容】
【手続補正５５】
【補正対象書類名】明細書
【補正対象項目名】００７０
【補正方法】削除
【補正の内容】
【手続補正５６】
【補正対象書類名】明細書
【補正対象項目名】００７１
【補正方法】削除
【補正の内容】
【手続補正５７】
【補正対象書類名】明細書
【補正対象項目名】００７２
【補正方法】削除
【補正の内容】
【手続補正５８】
【補正対象書類名】明細書
【補正対象項目名】００７３
【補正方法】削除
【補正の内容】
【手続補正５９】
【補正対象書類名】明細書
【補正対象項目名】００７４

【補正方法】削除
【補正の内容】
【手続補正６０】
【補正対象書類名】明細書
【補正対象項目名】００７５
【補正方法】削除
【補正の内容】
【手続補正６１】
【補正対象書類名】明細書
【補正対象項目名】００７６
【補正方法】削除
【補正の内容】
【手続補正６２】
【補正対象書類名】明細書
【補正対象項目名】００７７
【補正方法】削除
【補正の内容】
【手続補正６３】
【補正対象書類名】明細書
【補正対象項目名】００７８
【補正方法】削除
【補正の内容】
【手続補正６４】
【補正対象書類名】明細書
【補正対象項目名】００７９
【補正方法】削除
【補正の内容】
【手続補正６５】
【補正対象書類名】明細書
【補正対象項目名】００８０
【補正方法】削除
【補正の内容】
【手続補正６６】
【補正対象書類名】明細書
【補正対象項目名】００８１
【補正方法】削除
【補正の内容】
【手続補正６７】
【補正対象書類名】明細書
【補正対象項目名】００８２
【補正方法】削除
【補正の内容】
【手続補正６８】
【補正対象書類名】明細書
【補正対象項目名】００８３
【補正方法】削除
【補正の内容】
【手続補正６９】
【補正対象書類名】明細書
【補正対象項目名】００８４

【補正方法】削除
【補正の内容】
【手続補正７０】
【補正対象書類名】明細書
【補正対象項目名】００８５
【補正方法】削除
【補正の内容】
【手続補正７１】
【補正対象書類名】明細書
【補正対象項目名】００８６
【補正方法】削除
【補正の内容】
【手続補正７２】
【補正対象書類名】明細書
【補正対象項目名】００８７
【補正方法】削除
【補正の内容】
【手続補正７３】
【補正対象書類名】明細書
【補正対象項目名】００８８
【補正方法】削除
【補正の内容】